



دانشگاه صنعتی شریف

دانشکده مهندسی کامپیوتر

# گزارش کار آزمایشگاه آزمایشگاه شبکه‌های کامپیوتری

گزارش آزمایش شماره ۳

(آشنایی پیشرفته با نرم‌افزار Wireshark، نحوه تنظیم Server DNS)

۴

شماره گروه:

ارشیا یوسف‌نیا (۴۰۱۱۱۰۴۱۵)

گروه:

محمدفرحان بهرامی (۴۰۱۱۰۵۷۲۹)

امیرمهدی دارایی (۹۹۱۰۵۴۳۱)

دکتر صفایی

استاد درس:

تابستان ۱۴۰۴

تاریخ:

## فهرست مطالب

۱	۱	wireshark
۱	۱.۱	بازیابی کپچا
۲	۲.۱	سوال ها
۲	۱.۲.۱	
۲	۲.۲.۱	
۳	۲	راه اندازی DNS
۳	۱.۲	سناریو آزمایش
۸	۲.۲	پرسش ها
۸	۱.۲.۲	
۸	۲.۲.۲	

## لیست تصاویر

۱	باز کردن فایل و وارد کردن فایل نشست در بخش TLS	۱
۱	اعمال فیلتر در نمایش و خروجی گرفتن از فایل‌های رمزگشایی شده	۲
۱	کپی‌چای استخراج شده از فایل بسته‌ها	۳
۴	تنظیمات اصلی منطقه و رکوردهای معکوس، نوع آنها و محل فایل رکوردها	۴
۴	تنظیمات اصلی منطقه و رکوردهای معکوس، نوع آنها و محل فایل رکوردها	۵
۵	وارد کردن رکوردهای اصلی، سرور نام، آدرس آیپی، و نام‌های مستعار	۶
۵	وارد کردن رکوردها برای پرسش‌های معکوس	۷
۶	آماده کردن سرویس bind برای در نظر گرفته شدن در سوال‌ها	۸
۷	پرسش و پاسخ‌های مستقیم با nslookup	۹
۸	پرسش و پاسخ‌های وارونه با nslookup	۱۰
۸	پرسش و پاسخ‌های nslookup و بسته‌های ردگیری شده نرم‌افزار wireshark از این ارتباط	۱۱
۹	یک پرسمان با نوع رکورد A	۱۲
۹	یک پرسمان با نوع رکورد PTR	۱۳
۹	یک پرسمان با نوع رکورد AAAA	۱۴

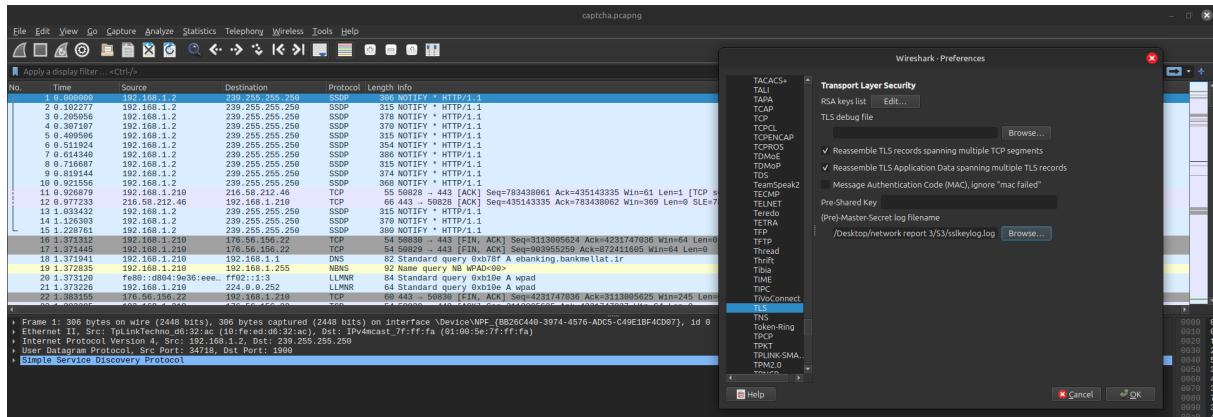
## لیست جداول

۱	ابزارهای آماری در Wireshark . . . . .	۲
۲	ویژگی‌های تحلیل RTP در Wireshark . . . . .	۳

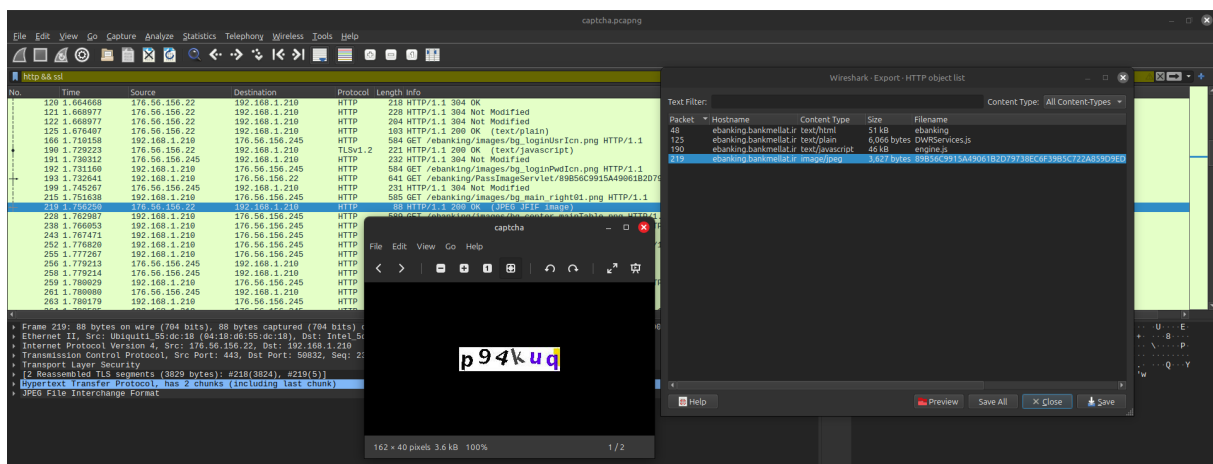
# wireshark ۱

## ۱.۱ بازیابی کپچا

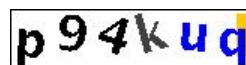
فایل مورد نظر را در نرم افزار باز می کنیم، در ادامه طبق شکل ۱ فایل رمز جلسه را در قسمت پروتکل TLS وارد می کنیم تا بتوانیم بسته های رمز شده را رمزگشایی کنیم. در نهایت با فیلتر موجود در شکل ۲ تنها این پیام ها را نشان می دهیم و فایل ها را از این پیام ها خروجی می گیریم. در شکل ۳ این فایل ها و حاصل کار آمده. شکل ۳ هم کد کپچا را جداگانه نشان می دهد. پس کد امنیتی p94kuq بوده.



شکل ۱: باز کردن فایل و وارد کردن نشست در بخش TLS



شکل ۲: اعمال فیلتر در نمایش و خروجی گرفتن از فایل های رمزگشایی شده



شکل ۳: کپچای استخراج شده از فایل بسته ها

## ۲.۱ سوال‌ها

### ۱.۲.۱

Wireshark دسترسی به اطلاعات آماری بسته‌ها را از طریق منوی "Statistics" فراهم می‌کند. این ابزارها برای تحلیل ترافیک شبکه، حتی در شرایطی که کلید جلسه برای بسته‌های رمزنگاری شده در دسترس نیست، بسیار مفید هستند. بر اساس مستندات Wireshark، ابزارهای آماری شامل مواردی که در جدول ۱ آمده هستند. این ابزارها به

ابزار آماری	توضیحات	کاربردها
Protocol Hierarchy	نمایش سلسله مراتبی از پروتکل‌ها و درصد استفاده هر کدام	تحلیل توزیع پروتکل‌ها و شناسایی ترافیک غالب
Conversations	لیست گفتگوها (ترافیک بین دو نقطه پایانی)	ردیابی الگوهای ارتباطی و شناسایی ناهنجاری‌ها
Endpoints	لیست نقاط پایانی (ترافیک به و از یک آدرس)	شناسایی دستگاه‌های فعال و ارزیابی حجم ترافیک
Packet Lengths	تحلیل توزیع اندازه بسته‌ها	شناسایی بسته‌های غیرمعمول و بهینه‌سازی شبکه
I/O Graphs	نمودارهای سفارشی برای نمایش ترافیک در طول زمان (مثلاً تعداد بسته‌ها)	مشاهده روندها و عیب‌یابی مشکلات عملکرد
Service Response Time	اندازه‌گیری زمان بین درخواست و پاسخ برای خدمات	ارزیابی تأخیر برنامه‌ها و اطمینان از کارایی

جدول ۱: ابزارهای آماری در Wireshark

کاربران اجازه می‌دهند بدون نیاز به رمزگشایی محتوای بسته‌ها، الگوهای ترافیک را تحلیل کنند. برای نمونه، اگر کلید جلسه برای بسته‌های رمزنگاری شده (مانند TLS) در دسترس نباشد، همچنان می‌توان حجم داده‌ها، فرکانس ارتباطات و پروتکل‌های استفاده شده را بررسی کرد. این قابلیت برای عیب‌یابی شبکه، برنامه‌ریزی ظرفیت و نظارت امنیتی بسیار مفید است.

در مورد رمزگشایی TLS، Wireshark برای رمزگشایی نیاز به کلیدهای خاصی مانند فایل لاگ کلید (Key Log File)، کلید خصوصی RSA یا کلید پیش‌اشتراکی (PSK) دارد. بدون این کلیدها، رمزگشایی ممکن نیست، اما ابزارهای آماری همچنان قابل استفاده هستند و اطلاعات ارزشمندی دارند. مراجع این بخش [۱، ۲] است.

### ۲.۲.۱

پروتکل RTP (Real-time Transport Protocol) یک پروتکل استاندارد برای انتقال داده‌های بی‌درنگ مانند صدا و ویدیو از طریق شبکه‌های IP است. این پروتکل معمولاً بر روی UDP اجرا می‌شود و برای کاربردهایی مانند VoIP، پخش زنده و کنفرانس ویدیویی استفاده می‌شود. RTP همراه با پروتکل کنترل RTCP برای نظارت بر تحویل داده‌ها کار می‌کند. Wireshark ابزارهای پیشرفته‌ای برای تحلیل ترافیک RTP ارائه می‌دهد که در جدول ۲ به آنها اشاره شده است.

این ابزارها به کاربران اجازه می‌دهند مشکلات رایج مانند جیتر بالا، از دست رفتن بسته‌ها یا تأخیر زیاد را شناسایی کنند. برای نمونه، تحلیل جیتر می‌تواند کیفیت تماس‌های صوتی را ارزیابی کند، و ذخیره جریان‌های

ویژگی	توضیحات	جزئیات/یادداشت‌ها
تحلیل جریان RTP	تحلیل آماری جریان‌های RTP از طریق منوی Telephony > RTP Show All Streams > ، شامل تأخیر، جیت، پهنای باند، از دست رفتن بسته‌ها و خطاهای توالی.	شامل نمودار برای نمایش جیت و تفاوت‌های بسته‌ها در طول زمان.
محاسبه جیت	محاسبه بر اساس RFC3550، فرمول: $J(i) = J(i-1) + ( D(i-1, i)  - J(i-1))/16$ ، نیاز به فرکانس نمونه‌برداری (مثلاً 8000 هرتز برای G.711).	مثال: PCMA G.711 با فرکانس 8000 هرتز، واحد 0.000125 ثانیه.
محاسبه پهنای باند	نمایش پهنای باند در سطح IP، شامل هدرهای IP (20 بایت) و UDP (8 بایت) در ثانیه اخیر.	رجوع به rtp_packet_analyse در تابع tap-rtp-common.c.
ذخیره جریان‌های صوتی RTP	ذخیره صدا در فایل Au از منوی تحلیل جریان RTP، پشتیبانی از کدک‌هایی با فرکانس 8000 هرتز (از نسخه 3.2.0، قبلاً فقط G.711).	گزینه‌ها: همگام‌سازی فایل، همگام‌سازی جریان، بدون همگام‌سازی.
پشتیبانی از کدک‌های دیگر	ذخیره در فرمت rtpdump برای کدک‌های دیگر، پخش با rtplay از rtptools، G.729 به دلیل هزینه مجوز پشتیبانی نمی‌شود.	مثال: پخش با JMstudio، آدرس IP محلی (نه 127.0.0.1).

جدول ۲: ویژگی‌های تحلیل RTP در Wireshark

صوتی برای بازتولید و تحلیل بیشتر مفید است. مستندات نشان می‌دهد که یک جیت کمتر از ۳۰ میلی‌ثانیه برای ترافیک صوتی قابل قبول است، و تأخیر یک‌طرفه کمتر از ۱۵۰ میلی‌ثانیه برای VoIP مناسب است. منبع [۳]

## ۲ راه‌اندازی DNS

این قسمت بر روی 'Xia' Linux Mint 22.1 انجام شده است. ابتدا bind9 را نصب می‌کنیم، همچنین در همین ابتدا دستورات کلیدی دیگر برای راه‌اندازی سرویس و بازنمایی آن آمده است.

```
sudo apt install bind9 bind9utils bind9-doc dnsutils
sudo systemctl start named
sudo systemctl restart named
```

### ۱.۲ سناریو آزمایش

یک منطقه به نام netlaba4.edu می‌سازیم. سرور نام یا nameserver آن را در ns.netlaba4.edu می‌گذاریم که ip برابر با 1.88.168.192 است. دو زیرمنطقه هم با نام‌های group1 و group2 به ترتیب با آدرس ip

برابر 11.88.168.192 و 22.88.168.192 است. هر دو زیردامنه نام مستعار هم دارند که جزییات آن در ادامه می‌آید. برای جستجوی معکوس هم رکوردها اضافه شده است. در شکل ۴ محتوای `/etc/bind/named.conf.local` که مربوط به منطقه و رکوردهای معکوس است آمده.

```

GNU nano 7.2 /etc/bind/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 "netlaba4.edu" {
    type master;
    file "/etc/bind/db.netlaba4.edu";
};

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

```

Help Write Out Where Is Cut Execute Location Undo Set Mark  
Exit Read File Replace Paste Justify Go To Line Redo Copy

شکل ۴: تنظیمات اصلی منطقه و رکوردهای معکوس، نوع آنها و محل فایل رکوردها.

در ادامه رکوردهای SOA و NS و A و CNAME را برای دو منطقه و دو زیردامنه خود در `/etc/bind/db.netlaba4.edu` وارد می‌کنیم، در شکل ۵ جزییات آمده است.

```

GNU nano 7.2 /etc/bind/db.netlaba4.edu *
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.netlaba4.edu. root.netlaba4.edu. (
    2      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns.netlaba4.edu.
@ IN A 192.168.88.1
@ IN AAAA ::1
ns IN A 192.168.88.1

group1 IN A 192.168.88.11
group2 IN A 192.168.88.22
group1canon IN CNAME group1
group2canon IN CNAME group2

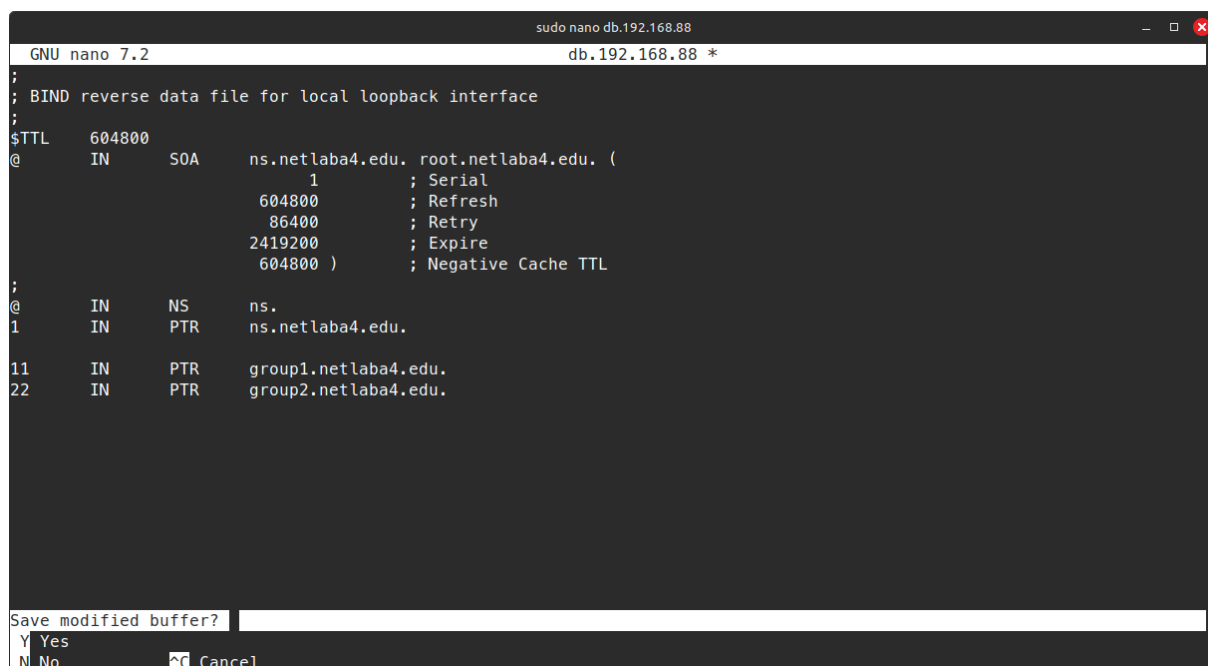
```

Save modified buffer? [Y] Yes [N] No [^C] Cancel

شکل ۵: تنظیمات اصلی منطقه و رکوردهای معکوس، نوع آنها و محل فایل رکوردها.



در شکل ۶ در `/etc/bind/db.88.168.192` به رکوردهای مربوط به پرسش‌های معکوس می‌پردازیم.

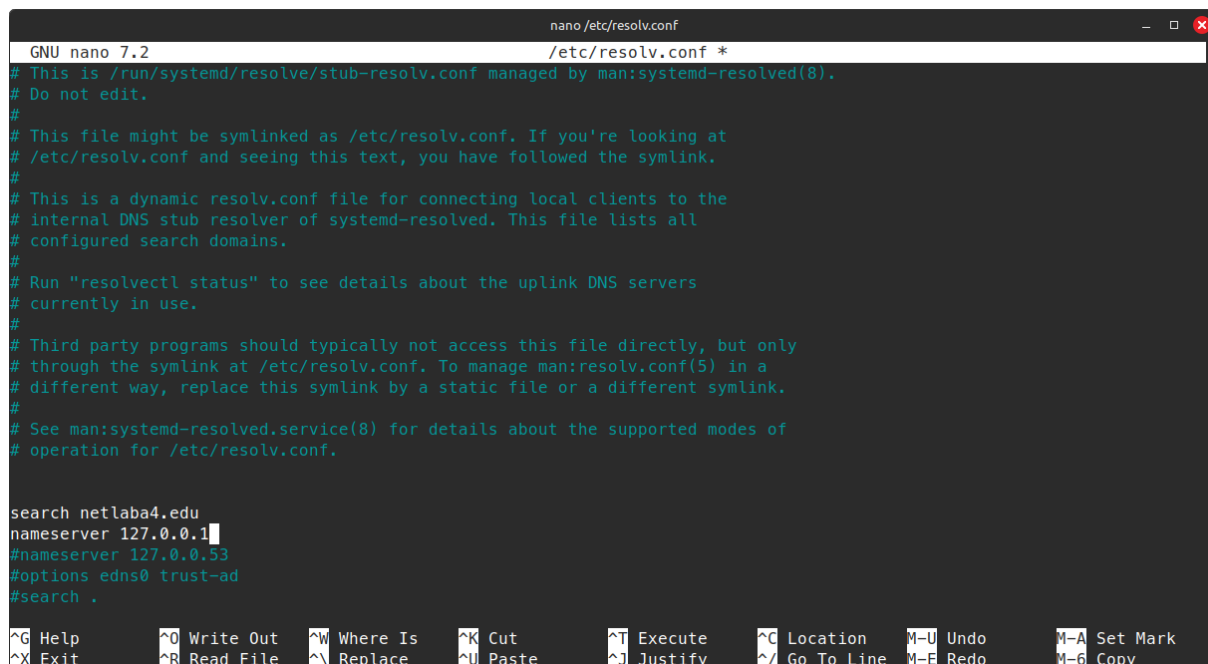


```
GNU nano 7.2 db.192.168.88 *
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.netlaba4.edu. root.netlaba4.edu. (
        1          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Negative Cache TTL
;
@ IN NS ns.
1 IN PTR ns.netlaba4.edu.
11 IN PTR group1.netlaba4.edu.
22 IN PTR group2.netlaba4.edu.

Save modified buffer?
Y Yes
N No ^C Cancel
```

شکل ۶: وارد کردن رکوردهای اصلی، سرور نام، آدرس آپی، و نام‌های مستعار

حالا باید کاری کنیم این سرویس در پرسش‌ها مورد توجه قرار گیرد. شکل ۷ در `/etc/resolv.conf` این کار را انجام می‌دهد.



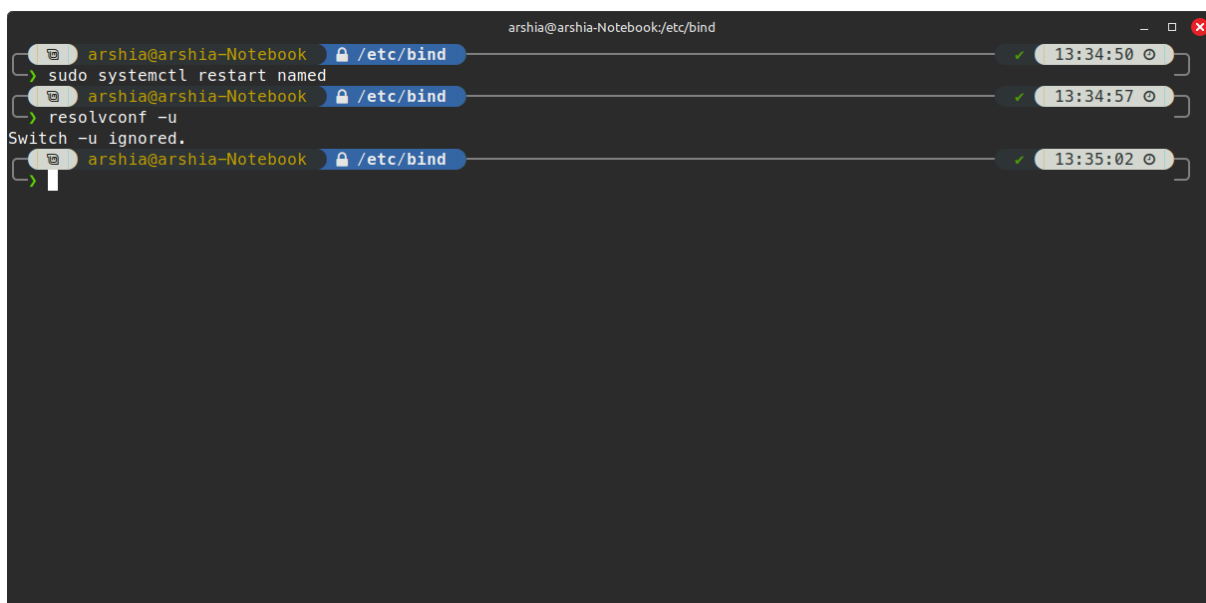
```
nano /etc/resolv.conf
GNU nano 7.2 /etc/resolv.conf *
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# 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.

search netlaba4.edu
nameserver 127.0.0.1
#nameserver 127.0.0.53
#options edns0 trust-ad
#search .

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo     M-A Set Mark
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo     M-6 Copy
```

شکل ۷: وارد کردن رکوردها برای پرسش‌های معکوس

در نهایت با دستورهای آماده در ابتدای این بخش سرویس ها را restart می کنیم که در شکل ۸ آمده است. در ادامه باید نتایج را آزمایش کنیم و همزمان نرم افزار wireshark را هم روی واسط loopback به حالت capture قرار می دهیم.



```
arshia@arshia-Notebook/etc/bind
> sudo systemctl restart named
arshia@arshia-Notebook/etc/bind
> resolvconf -u
Switch -u ignored.
arshia@arshia-Notebook/etc/bind
>
```

شکل ۸: آماده کردن سرویس bind برای در نظر گرفته شدن در سوال ها

پرسش های مستقیم با nslookup در شکل ۹ و پرسش های معکوس در شکل ۱۰ به همراه پاسخ ها آمده است.

```
arshia@arshia-Notebook:/etc/bind
> nslookup netlaba4.edu
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   netlaba4.edu
Address: 192.168.88.1
Name:   netlaba4.edu
Address: ::1

arshia@arshia-Notebook:/etc/bind
> nslookup ns.netlaba4.edu
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   ns.netlaba4.edu
Address: 192.168.88.1

arshia@arshia-Notebook:/etc/bind
> nslookup group1.netlaba4.edu
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   group1.netlaba4.edu
Address: 192.168.88.11

arshia@arshia-Notebook:/etc/bind
> nslookup group2.netlaba4.edu
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   group2.netlaba4.edu
Address: 192.168.88.22

arshia@arshia-Notebook:/etc/bind
> nslookup group1canon.netlaba4.edu
Server:      127.0.0.1
Address:     127.0.0.1#53

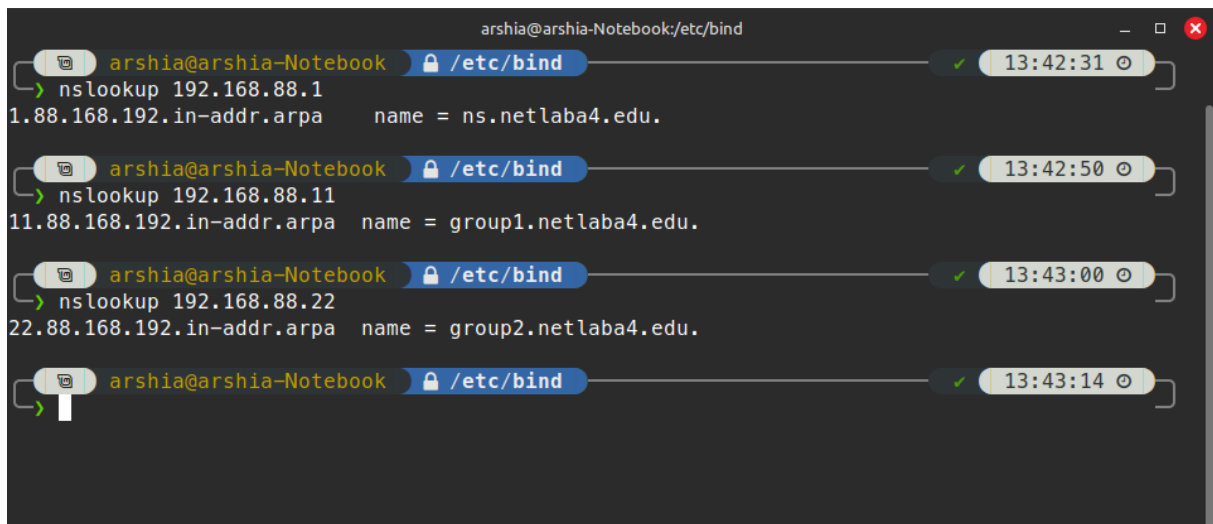
group1canon.netlaba4.edu    canonical name = group1.netlaba4.edu.
Name:   group1.netlaba4.edu
Address: 192.168.88.11

arshia@arshia-Notebook:/etc/bind
> nslookup group2canon.netlaba4.edu
Server:      127.0.0.1
Address:     127.0.0.1#53

group2canon.netlaba4.edu    canonical name = group2.netlaba4.edu.
Name:   group2.netlaba4.edu
Address: 192.168.88.22

arshia@arshia-Notebook:/etc/bind
>
```

شکل ۹: پرسش و پاسخ‌های مستقیم با nslookup

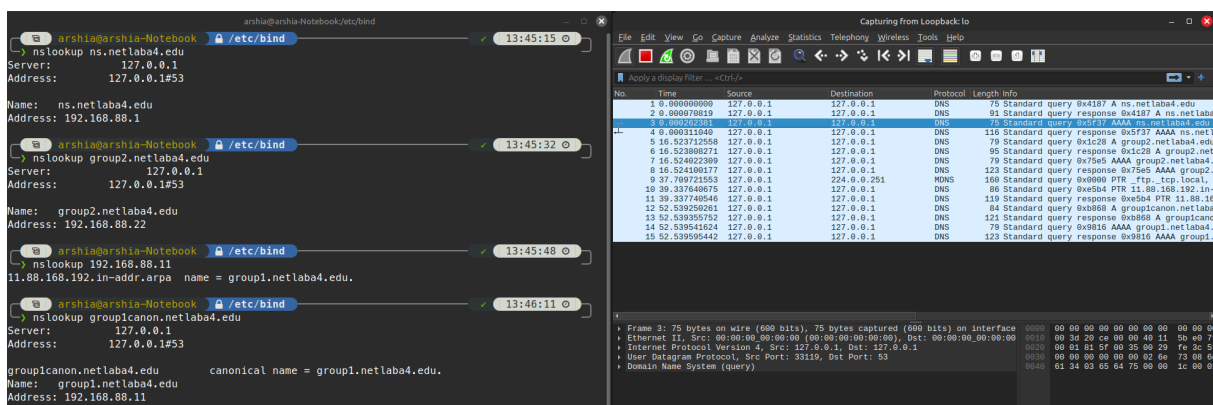


شکل ۱۰: پرسش و پاسخ‌های وارونه با nslookup

## ۲.۲ پرسش‌ها

### ۱.۲.۲

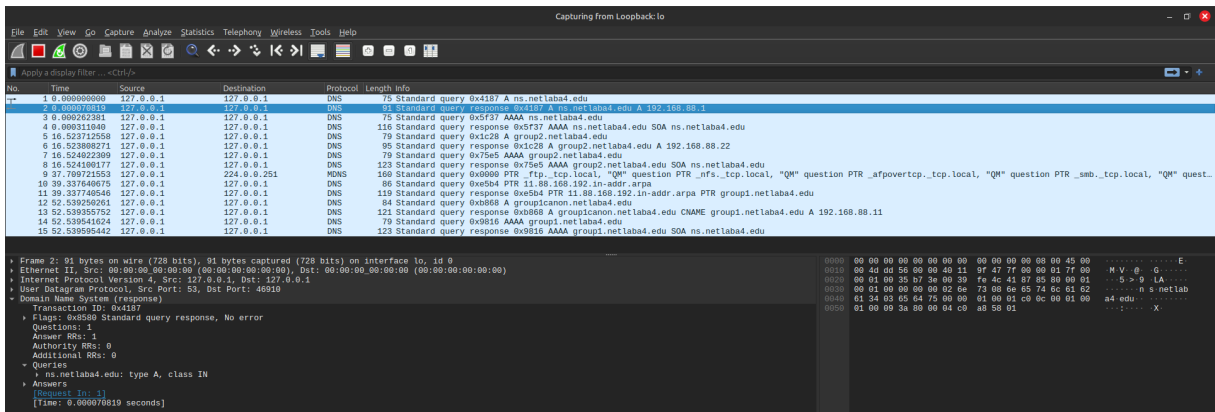
همانطور که در شکل ۱۱ آمده، متناظر با هر پرسش با nslookup یک بسته با پروتکل DNS ارسال شده و به ازای جواب آن هم یک بسته آمده است که رفتار مورد انتظار DNS است.



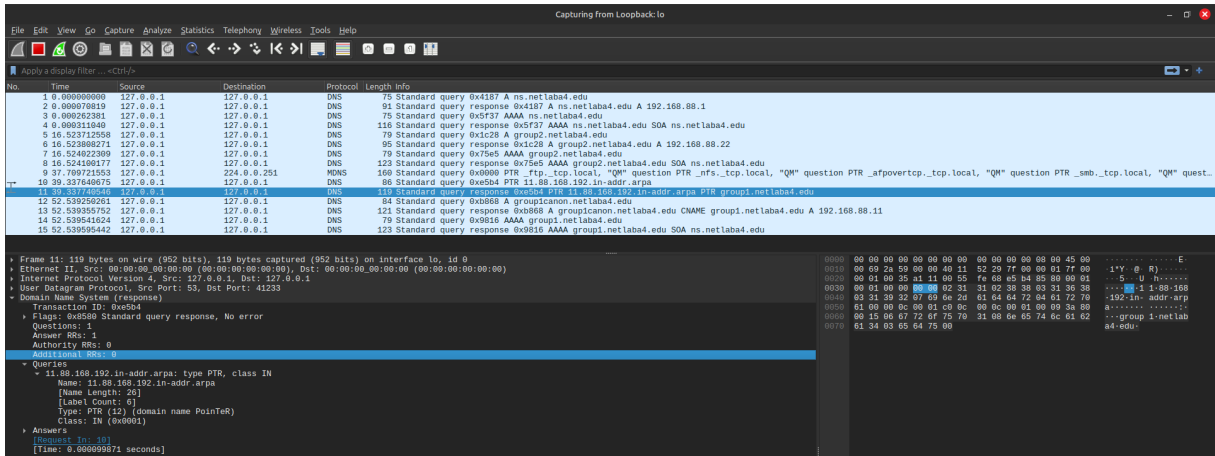
شکل ۱۱: پرسش و پاسخ‌های nslookup و بسته‌های ردگیری شده نرم‌افزار wireshark از این ارتباط

### ۲.۲.۲

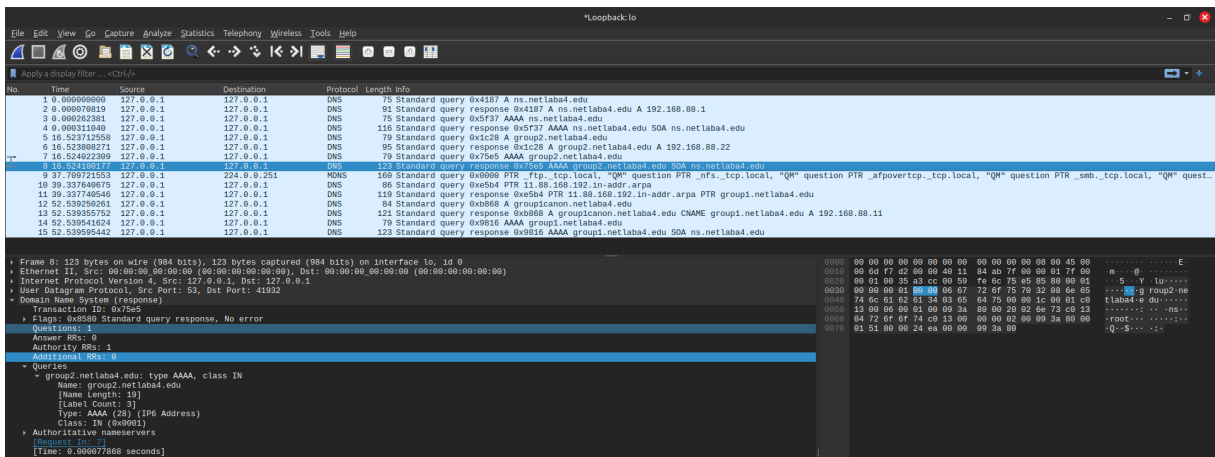
در شکل‌های ۱۲، ۱۳، و ۱۴ نوع از پرسش‌های مختلف را آورده‌ایم، پرسش‌های مستقیم به دنبال آدرس آییی بوده‌اند که بیشتر نسخه ۴ بوده، پس در پرسش و پاسخ متناظر A آمده است، به همین ترتیب برای آییی نسخه ۶ نیز AAAA آمده است. در نهایت برای پرسش‌های وارونه که به دنبال آییی از روی نام هستند هم نوع PTR یا domain name Pointer آمده است.



شکل ۱۲: یک پرسمان با نوع رکورد A



شکل ۱۳: یک پرسمان با نوع رکورد PTR



شکل ۱۴: یک پرسمان با نوع رکورد AAAA

- [١] URL: [https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChUseStatisticsMenuSection.html](https://www.wireshark.org/docs/wsug_html_chunked/ChUseStatisticsMenuSection.html).
- [٢] URL: <https://wiki.wireshark.org/TLS>.
- [٣] URL: [https://wiki.wireshark.org/RTP\\_statistics](https://wiki.wireshark.org/RTP_statistics).