

به نام خدا

ازمایشگاه شبکه های کامپیوتری



گزارش آزمایش سوم

گروه اول

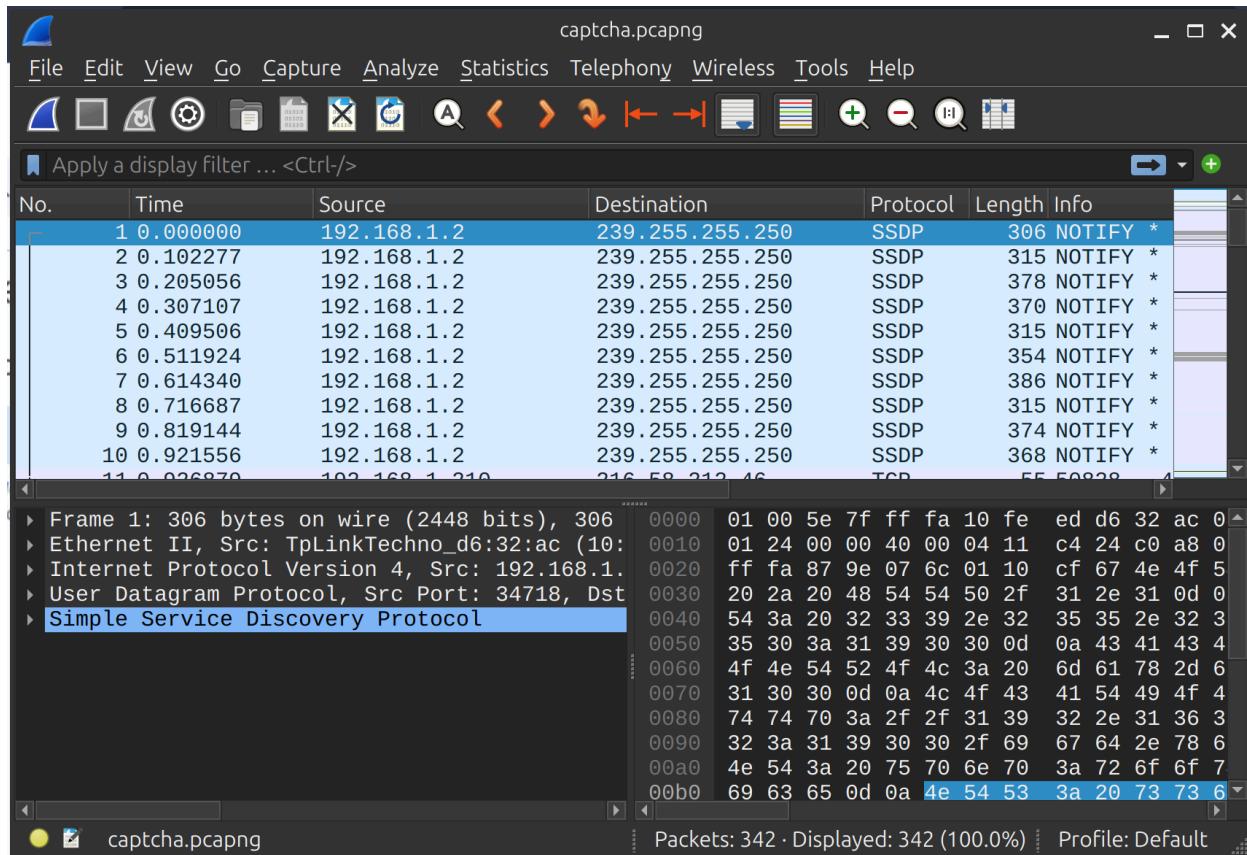
مهدی محمدی 400105239

ملیکا علیزاده 401106255

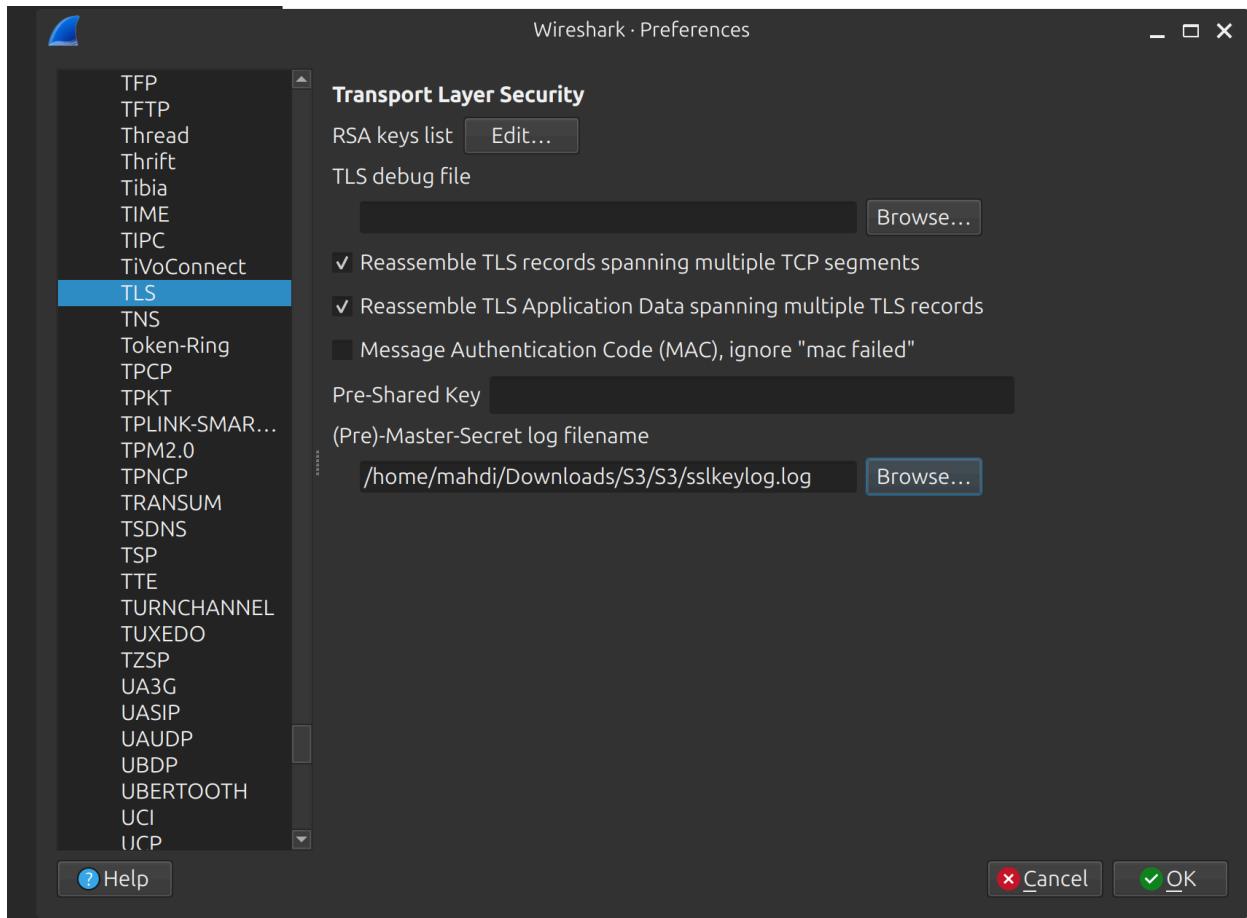
معین آعلی 401105561

## بخش اول

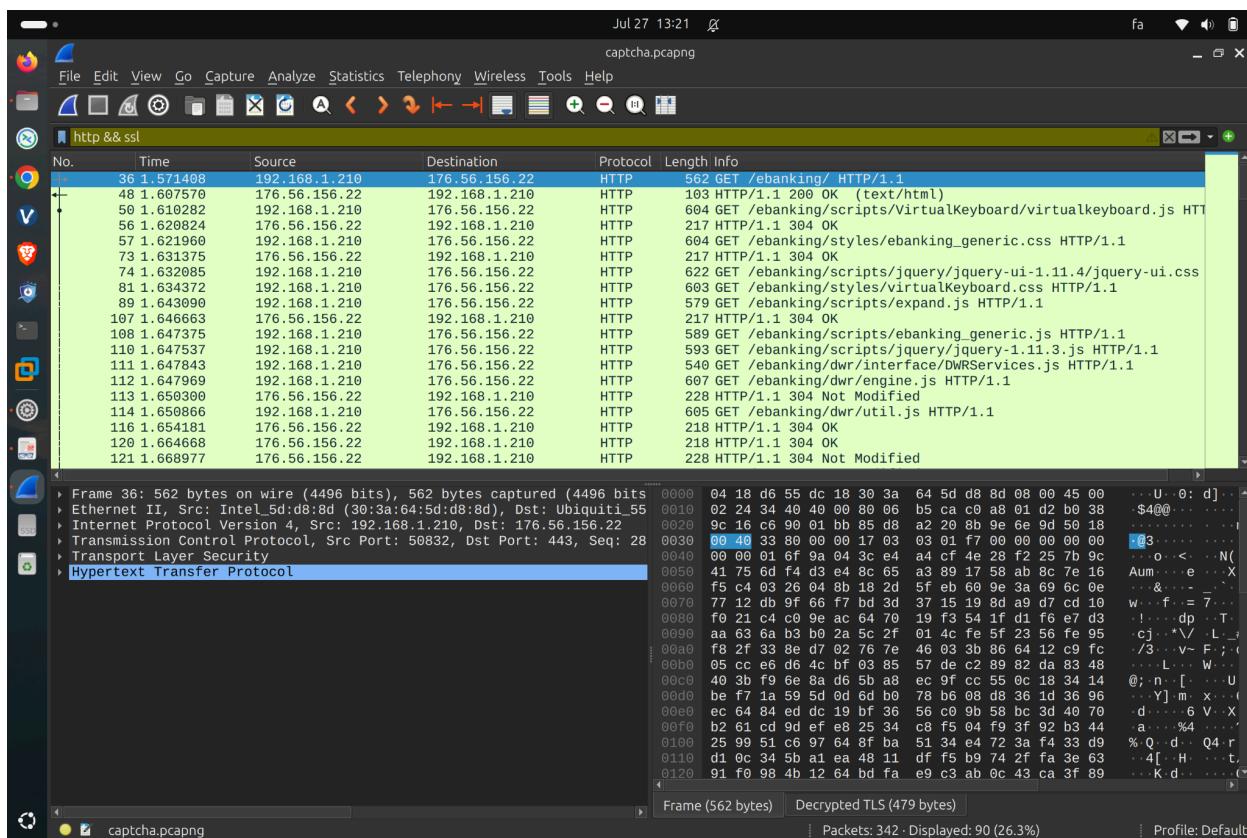
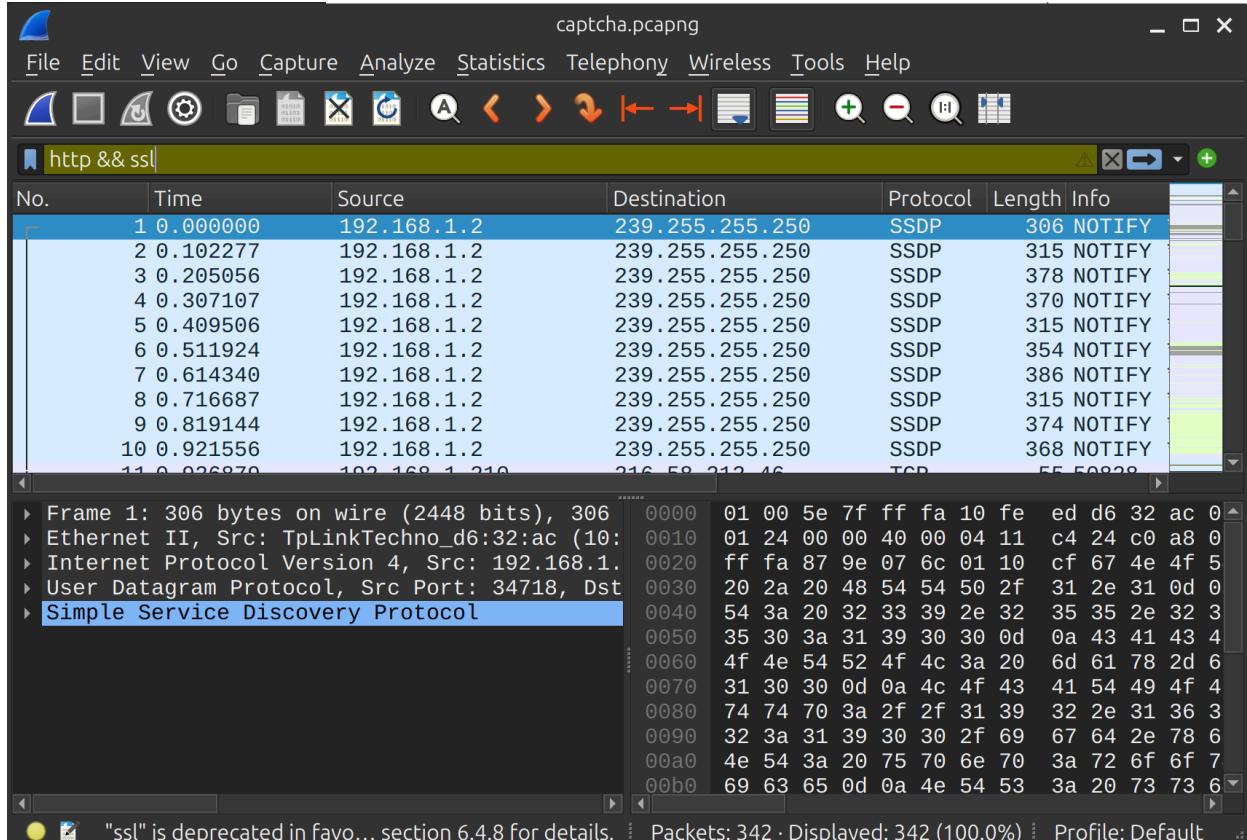
ابتدا از فایل pcap را باز میکنیم.



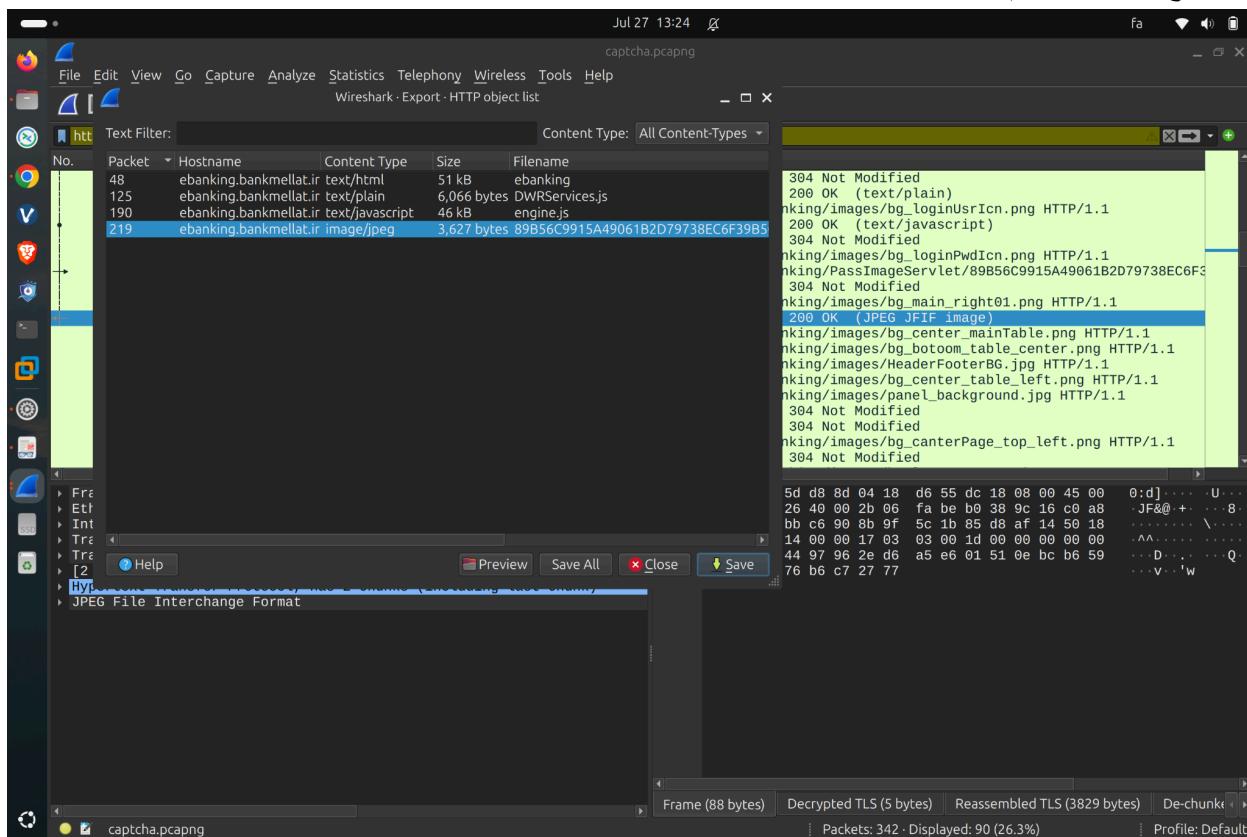
سپس با رفتن به قسمت TLS کلید داده شده را وارد میکنیم.



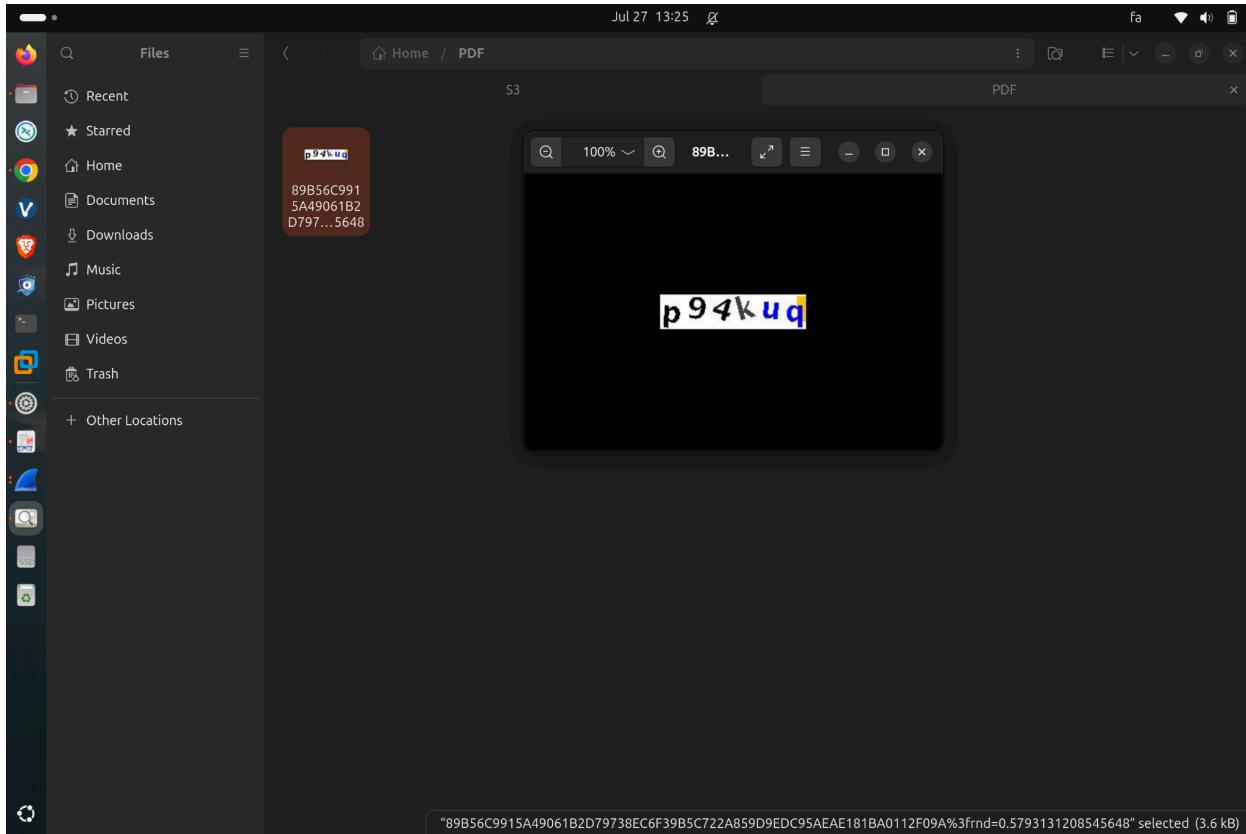
فیلتر مدنظر را اعمال میکنیم.



فایل ایمیج را ذخیره میکنیم.



ایمیج را برای اطمینان از صحت ذخیره شدن در فایل سیستم باز میکنیم.



### سوال 1:

در نرم افزار Wireshark، اطلاعات آماری بسته ها از طریق منوی Statistics در نوار ابزار بالا در دسترس قرار می گیرد. از مهمترین ابزار های آماری Wireshark می توان به موارد زیر اشاره کرد:

- اطلاعات کلی مانند تعداد کل بسته ها، مدت زمان ضبط، سرعت متوسط شبکه و غیره را نمایش می دهد.

- آماری از پروتکل های استفاده شده در بسته ها را به صورت سلسله مراتبی نمایش می دهد.

- لیستی از مکالمات (session) بین IP ها یا پورت ها و اطلاعاتی مانند تعداد بسته ها، اندازه، زمان شروع و پایان هر مکالمه.

- نمایش نموداری جریان داده در طول زمان.

- نمایش اطلاعات آماری مربوط به گره ها (End Points) از جمله تعداد بسته ها، بایت ها، و نقش آن ها در شبکه.

- ❖ کمک هایی که این اطلاعات به ما می کنند:

- تحلیل ترافیک شبکه: برای شناسایی نقاط پُر ترافیک یا اختلال در عملکرد.

- عیبیابی شبکه: برای کشف بسته های گم شده، تکراری یا خراب شده.

- شناسایی حملات یا فعالیت های مشکوک: مانند اسکن پورت یا حملات DoS.

- تحلیل رمزنگاری: مثلاً زمانی که کلید رمزنگاری TLS در دسترس نباشد، می توان با مشاهده مکالمات و آمار مربوط به بسته ها فهمید که چه مقدار داده رمزنگاری شده رد و بدل شده، ارتباطات در چه بازه های زمانی برقرار بوده اند و به صورت غیر مستقیم از الگوهای رفتاری تحلیل انجام داد.

اگر کلید جلسه TLS (مثلاً فایل Key Log) موجود نباشد و محتوای بسته ها رمزنگاری شده باشد، اطلاعات آماری همچنان می توانند در بررسی نوع فعالیت شبکه و ترافیک کلی مفید واقع شوند.

### سوال 2:

پروتکل Real-time Transport Protocol (RTP) یک پروتکل لایه انتقال است که برای انتقال داده های بلند نگ مانند صدا (Voice)، ویدئو (Video) یا دیگر داده های چند رسانه ای در بستر شبکه هایی مانند IP طراحی شده است.

## ویژگی‌های کلیدی RTP:

- استفاده از UDP به عنوان پروتکل زیرین (نه TCP).
- دارای شماره توالی (Sequence Number) برای تشخیص ترتیب بسته‌ها.
- دارای تایم‌استمپ (Timestamp) برای همزمانسازی داده‌ها.
- امکان استفاده در کنار RTCP برای کنترل جریان داده و دریافت بازخورد.

## ❖ نقش Wireshark در تحلیل RTP:

- می‌تواند بسته‌های RTP را به صورت خودکار شناسایی کند (در صورت وجود سیگنال‌گذاری مناسب مانند (SIP

### • از طریق منوی Telephony > RTP > Show All Streams می‌توان تمام جریان‌های RTP را دید.

- امکان پخش صدای استخراج شده از RTP وجود دارد (در تماس‌های VoIP مثلاً (SIP

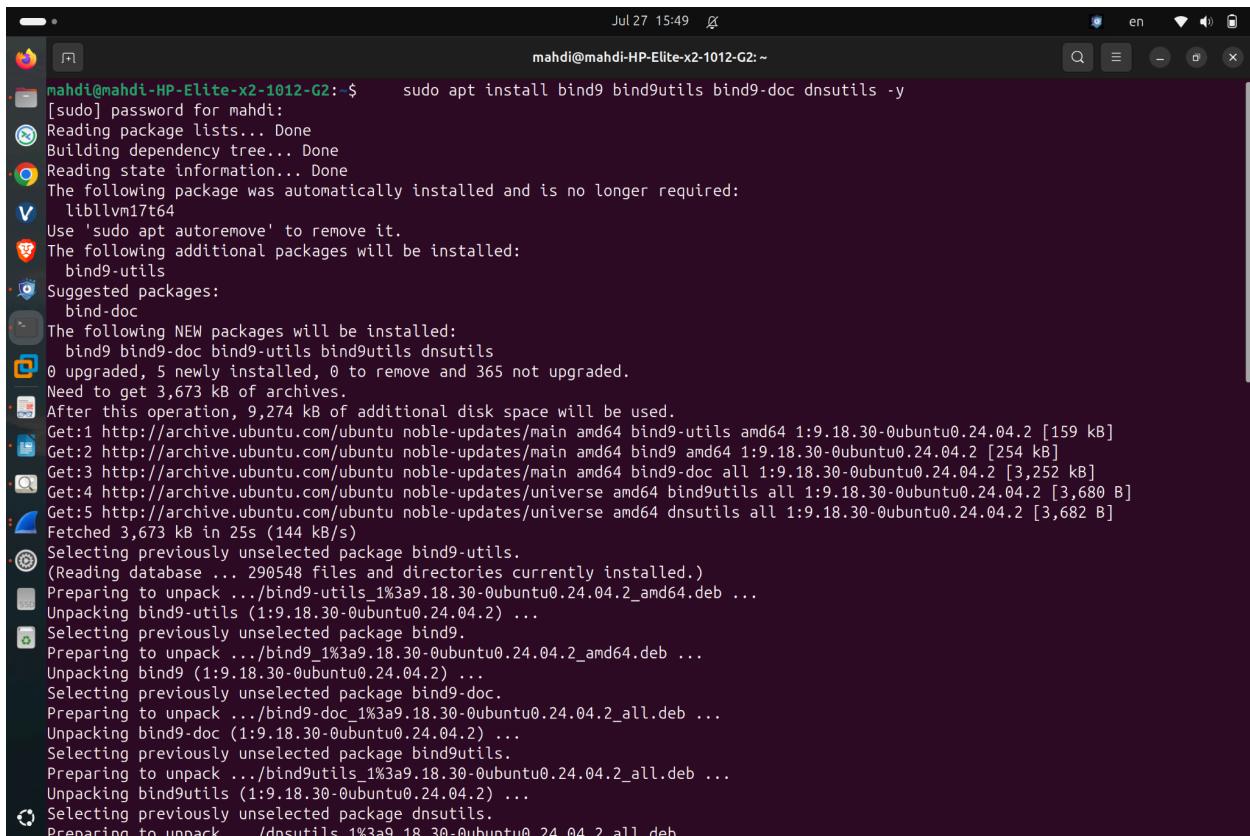
### • تحلیل پارامترهای مهم مانند jitter، delay، از دست رفتن بسته‌ها و ترتیب آن‌ها.

- Export RTP Stream: برای ذخیره‌سازی داده‌های صوتی به صورت فایل WAV و بررسی دقیق.

بنابراین Wireshark ابزار بسیار مؤثری برای تحلیل تماس‌های VoIP و بررسی کیفیت و سلامت جریان‌های RTP است.

## بخش دوم

ابتدا bind9 و سرویس‌های مربوط به آن را نصب می‌کنیم.



```
mahdi@mahdi-HP-Elite-x2-1012-G2:~$ sudo apt install bind9 bind9utils bind9-doc dnsutils -y
[sudo] password for mahdi:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  liblvm17t64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  bind9-utils
Suggested packages:
  bind-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils dnsutils
0 upgraded, 5 newly installed, 0 to remove and 365 not upgraded.
Need to get 3,673 kB of archives.
After this operation, 9,274 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-utils amd64 1:9.18.30-0ubuntu0.24.04.2 [159 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9 amd64 1:9.18.30-0ubuntu0.24.04.2 [254 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-doc all 1:9.18.30-0ubuntu0.24.04.2 [3,252 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 bind9utils all 1:9.18.30-0ubuntu0.24.04.2 [3,680 B]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 dnsutils all 1:9.18.30-0ubuntu0.24.04.2 [3,682 B]
Fetched 3,673 kB in 25s (144 kB/s)
Selecting previously unselected package bind9-utils.
(Reading database ... 290548 files and directories currently installed.)
Preparing to unpack .../bind9-utils_1%3a9.18.30-0ubuntu0.24.04.2_amd64.deb ...
Unpacking bind9-utils (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.18.30-0ubuntu0.24.04.2_amd64.deb ...
Unpacking bind9 (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package bind9-doc.
Preparing to unpack .../bind9-doc_1%3a9.18.30-0ubuntu0.24.04.2_all.deb ...
Unpacking bind9-doc (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package bind9utils.
Preparing to unpack .../bind9utils_1%3a9.18.30-0ubuntu0.24.04.2_all.deb ...
Unpacking bind9utils (1:9.18.30-0ubuntu0.24.04.2) ...
Selecting previously unselected package dnsutils.
Preparing to unpack .../dnsutils_1%3a9.18.30-0ubuntu0.24.04.2_all.deb ...
```

سپس از اجرای صحیح آن مطمئن می‌شویم.

```
mahdi@mahdi-HP-Elite-x2-1012-G2:~$ systemctl status bind9
● named.service - BIND Domain Name Server
  Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: en>
  Active: active (running) since Sun 2025-07-27 15:48:30 +0330; 56s ago
    Docs: man:named(8)
   Main PID: 9371 (named)
     Status: "running"
       Tasks: 14 (limit: 18876)
      Memory: 9.0M (peak: 9.5M)
        CPU: 201ms
      CGroup: /system.slice/named.service
              └─9371 /usr/sbin/named -f -u bind

Jul 27 15:49:06 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: no valid RRSIG resolving>
Jul 27 15:49:07 mahdi-HP-Elite-x2-1012-G2 named[9371]: broken trust chain resol>
mahdi@mahdi-HP-Elite-x2-1012-G2:~$
```

حال همانطور که در دستور کار آزمایش گفته شده، یک منطقه با نام [NeLab1.edu](http://NeLab1.edu) میسازیم و دو هاست گفته شده را تعریف میکنیم. فایل `/etc/bind/named.conf.local` را مشاهده میکنید.

```
// 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 "NetLab1.edu" {
    type master;
    file "/etc/bind/db.NetLab1.edu";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.1";
};

~
```

حال فایل `/etc/bind/db.NetLab1.edu` را میبینیم.

```
Jul 27 17:11  ✘
root@mahdi-HP-Elite-x2-1012-G2: /home/mahdi
$TTL 604800
@ IN SOA ns1.NetLab5.edu. admin.NetLab5.edu. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

; Name servers
@ IN NS ns1.NetLab5.edu.

; A records for hosts
ns1 IN A 192.168.1.100
group1 IN A 192.168.1.101
group2 IN A 192.168.1.102

; CNAME records (aliases)
www IN CNAME group1
ftp IN CNAME group2
~
~
```

همانطور که مشاهده میکنید، دو هاست group1 و group2 اضافه شده اند. همچنین برای هر هاست، یک CNAME تعریف شده است.

حال فایل /etc/bind/db.192.168.1 را مشاهده میکنیم. همانطور که میبینید، رکورد های PTR برای جستجوی معکوس(تبديل آدرس آپی به نام دامنه) اضافه شده اند.

پس از اعمال این تنظیمات، ابتدا از درستی سینتکس اطمینان حاصل کرده و سپس سرویس bind9 را ریستاart میکنیم تا تغییرات اعمال شوند.

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# sudo named-checkconf
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# sudo named-checkzone NetLab1.edu /etc/bind/db.NetLab1.edu
zone NetLab1.edu/IN: loaded serial 3
OK
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# sudo named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192.168.1
zone 1.168.192.in-addr.arpa/IN: loaded serial 3
OK
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# █
```

پس از این کار فایل /etc/resolv.conf را به شکل زیر تغییر میدهیم تا از سرویسی که خودمان اجرا کردیم به عنوان dns استفاده کند

حال صحت اجرای سرویس را چک میکنیم.

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# dig ns1.NetLab1.edu
; <>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <>> ns1.NetLab1.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11215
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a3c5d23df8bdd2870100000068862d8cb1532a78b0b90aef (good)
;; QUESTION SECTION:
;ns1.NetLab1.edu.           IN      A

;; ANSWER SECTION:
ns1.NetLab1.edu.       604800  IN      A      192.168.1.100

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Jul 27 17:15:48 +0330 2025
;; MSG SIZE  rcvd: 88

root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi#
```

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# dig group2.NetLab1.edu
; <>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <>> group2.NetLab1.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 5261
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: d27871768f946c00100000068862d723e6d5dc7ade85b42 (good)
;; QUESTION SECTION:
;group2.NetLab1.edu.      IN      A

;; ANSWER SECTION:
group2.NetLab1.edu.  604800  IN      A      192.168.1.102

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Jul 27 17:15:22 +0330 2025
;; MSG SIZE  rcvd: 91

root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi#
```

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# dig group1.NetLab1.edu
; <>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <>> group1.NetLab1.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 48845
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: 5b571e5b78f5391e0100000068862db34aebdad8c74e8e14 (good)
;; QUESTION SECTION:
;group1.NetLab1.edu.      IN      A

;; ANSWER SECTION:
group1.NetLab1.edu.  604800  IN      A      192.168.1.101

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Jul 27 17:16:27 +0330 2025
;; MSG SIZE  rcvd: 91

root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi#
```

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# dig www.NetLab1.edu

; <>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <>> www.NetLab1.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2863
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a5e14dbff733821d0100000068862dd325fdbd7fc3a90df56 (good)
;; QUESTION SECTION:
;www.NetLab1.edu.           IN      A

;; ANSWER SECTION:
www.NetLab1.edu.      604800  IN      CNAME   group1.NetLab1.edu.
group1.NetLab1.edu.    604800  IN      A       192.168.1.101

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Jul 27 17:16:59 +0330 2025
;; MSG SIZE  rcvd: 109

root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi#
```

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# dig -x 192.168.1.101

; <>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <>> -x 192.168.1.101
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12625
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8d89db2058448b490100000068862df715a7bb4b7eb335f9 (good)
;; QUESTION SECTION:
;101.1.168.192.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
101.1.168.192.in-addr.arpa. 604800 IN  PTR      group1.NetLab1.edu.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Jul 27 17:17:35 +0330 2025
;; MSG SIZE  rcvd: 115

root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi#
```

```
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi# nslookup ftp.NetLab1.edu
Server:      127.0.0.1
Address:      127.0.0.1#53

ftp.NetLab1.edu canonical name = group2.NetLab1.edu.
Name:      group2.NetLab1.edu
Address:    192.168.1.102

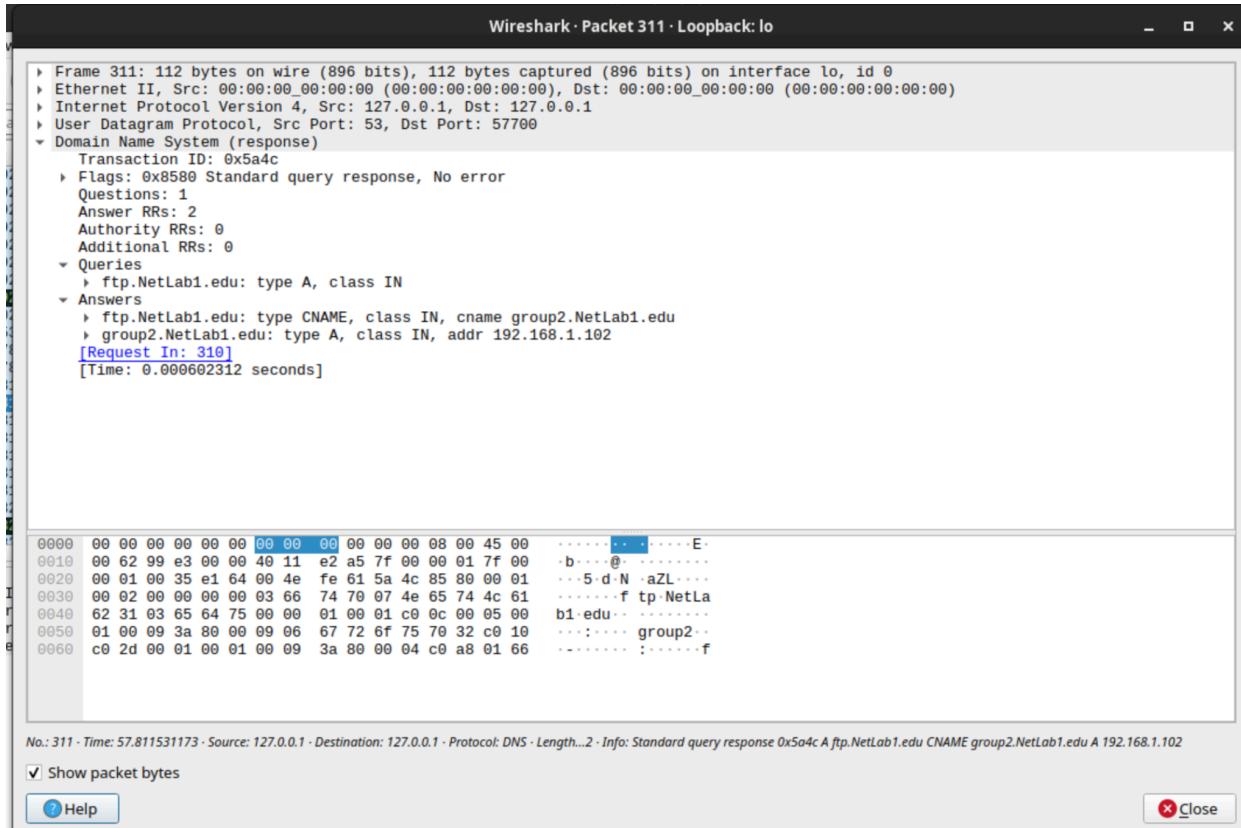
root@mahdi-HP-Elite-x2-1012-G2:/home/mahdi#
```

پکت های منتقل شده در اثر nslookup بالا را مشاهده میکنید. توجه کنید که پکت چهارم مربوط به دستور بالا نیست، بلکه یک درخواست جداگانه برای [waa-pa.googleapis.com](http://waa-pa.googleapis.com) ارسال شده که همانطور که انتظار میرود، fail شده است چراکه dns ما همچین آدرسی را ندارد و server resolve نمیکند.

همانطور که میبینید ابتدا یک درخواست (standard query) برای [ftp.NetLab1.edu](http://ftp.NetLab1.edu) ارسال شده است، سپس پاسخ این درخواست که نام دامنه ایست که این نام مستعار به آن اشاده میکند، ارسال گردیده است (CNAME). سپس یک درخواست برای [group2.NetLab1.com](http://group2.NetLab1.com) ارسال شده که در پاسخ این نام دامنه به آدرس آبی مربوطه مپ شده است (A record).

309 57.810081099	127.0.0.1	127.0.0.1	DNS	81 Standard query 0x1c35 HTTPS waa-pa.googleapis.com
310 57.810928061	127.0.0.1	127.0.0.1	DNS	75 Standard query 0x5a4c A ftp.NetLab1.edu
311 57.811531173	127.0.0.1	127.0.0.1	DNS	112 Standard query response 0x5a4c A ftp.NetLab1.edu CNAME group2.NetLab1.edu A 192.168.1.102
312 57.812924382	127.0.0.1	127.0.0.1	DNS	78 Standard query 0x5702 AAAA group2.NetLab1.edu
313 57.813150643	127.0.0.1	127.0.0.1	DNS	81 Standard query response 0x70c7 Server failure A waa-pa.googleapis.com
314 57.813810460	127.0.0.1	127.0.0.1	DNS	135 Standard query response 0x5702 AAAA group2.NetLab1.edu SOA ns1.NetLab5.edu

پکت سلکت شده در تصویر را با جزئیات بیشتر در تصویر زیر میبینید.



رکورد هایی که تعریف کردیم چهار نوع resource record مختلف بودند. رکورد [ns1.NetLab1.edu](#) از نوع NS است. رکورد های مربوط به هاست ها، که group1 و group2 را به آدرس آپی های مربوطه مپ میکرند از نوع A record بودند. نام های مستعاری که تعریف کردیم (www برای group1 و ftp برای group2) از نوع CNAME بودند. رکورد هایی که برای جستجوی معکوس تعریف کردیم که آدرس آپی را به نام دامنه مپ میکرند از نوع PTR بودند. تعریف زون هم (Start Of Authority) است.