به نام خدا

# آزمایشگاه شبکه‌های کامپیوتری

**گزارش آزمایش سوم**

استاد:

**دکتر حمید بیگی**


نویسندگان :

**محمدهومان کشوری**

**هیربد بهنام**

**علی نظری**

شماره دانشجویی :

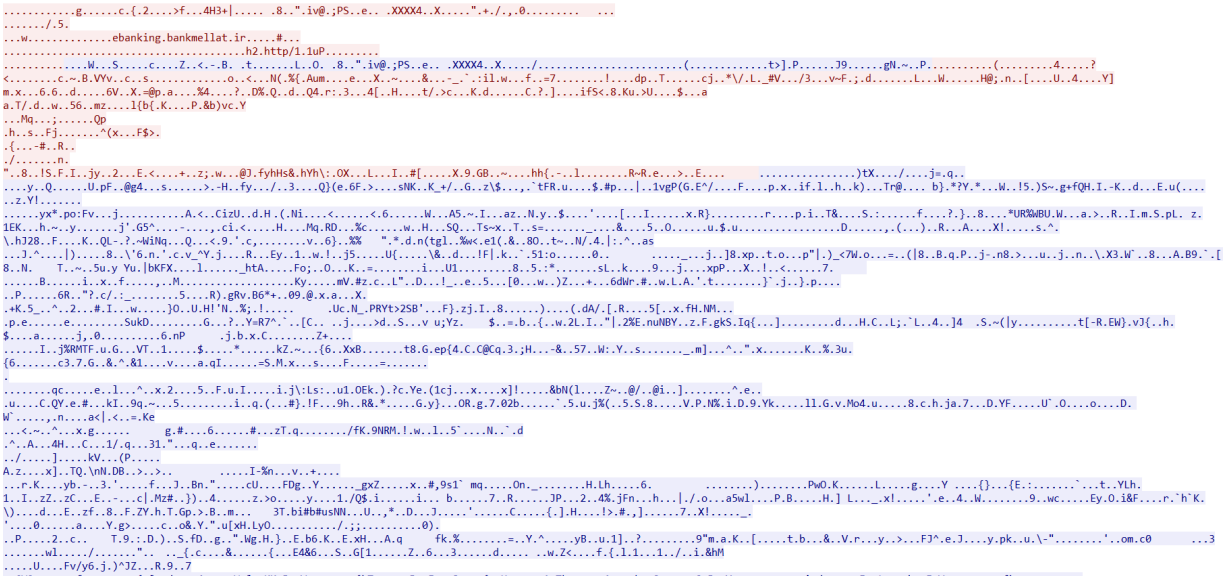
**99105667**

**99171333**

**99102401**

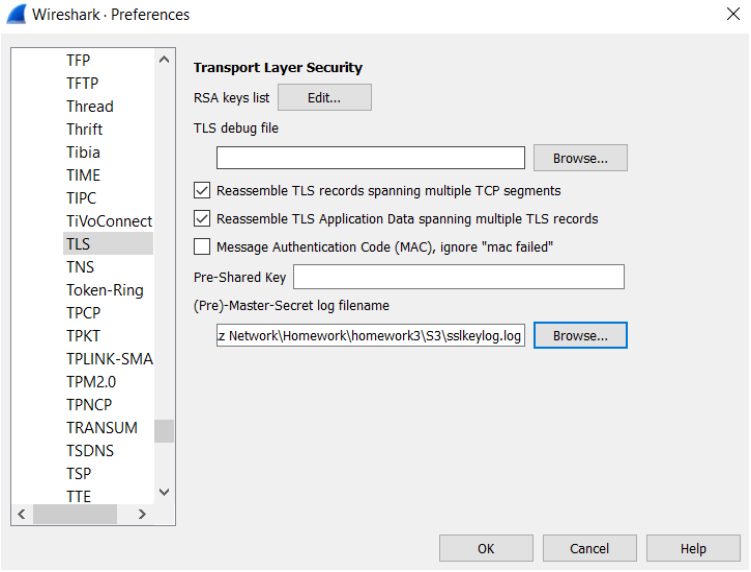
# راه حل

می‌دانیم که tls همان tcp رمزگذاری شده است پس ابتدا با زدن دستور follow tcp stream، پیام‌های رد و بدل شده را مشاهده می‌کنیم.



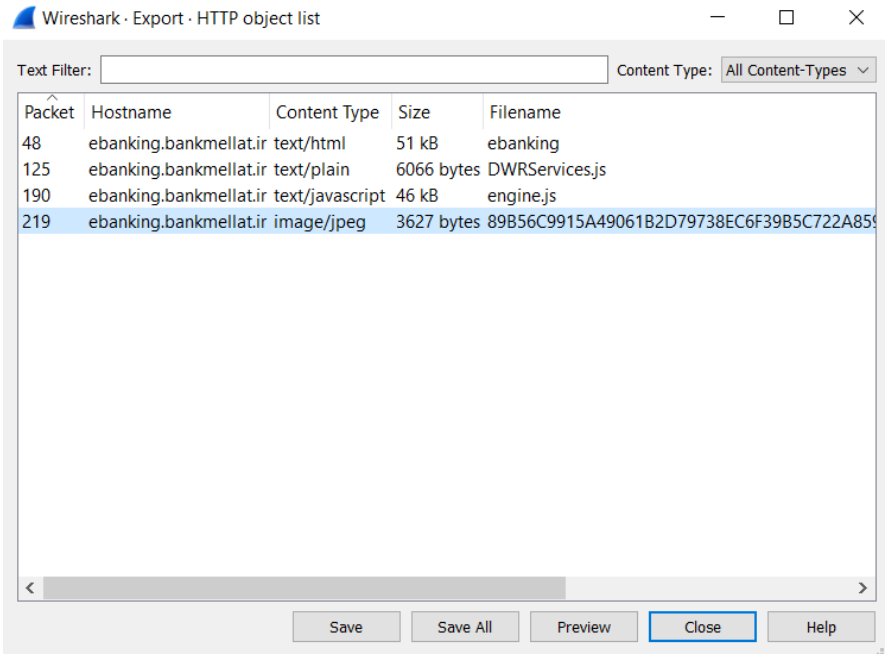
به وضوح مشخص است که پیام‌ها رمزگذاری شده و human readable نیستند پس نیاز به دیکود کردن آنها داریم.

طبق [این منبع](#) به این دلیل که ssl خالی عملا deprecated شده است، در نسخه‌های جدید wireshark دیگر در قسمت protocols وجود ندارد پس باید از گزینه tls استفاده کنیم.



http && tls

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 36 | 1.571408 | 192.168.1.210 | 176.56.156.22 | HTTP | 562 | GET /ebanking/ HTTP/1.1 |
| 48 | 1.607570 | 176.56.156.22 | 192.168.1.210 | HTTP | 103 | HTTP/1.1 200 OK (text/html) |
| 50 | 1.610282 | 192.168.1.210 | 176.56.156.22 | HTTP | 604 | GET /ebanking/scripts/VirtualKeyboard/virtualkeyboard.js HTTP/1.1 |
| 56 | 1.620824 | 176.56.156.22 | 192.168.1.210 | HTTP | 217 | HTTP/1.1 304 OK |
| 57 | 1.621960 | 192.168.1.210 | 176.56.156.22 | HTTP | 604 | GET /ebanking/styles/ebanking_generic.css HTTP/1.1 |
| 73 | 1.631375 | 176.56.156.22 | 192.168.1.210 | HTTP | 217 | HTTP/1.1 304 OK |
| 74 | 1.632085 | 192.168.1.210 | 176.56.156.22 | HTTP | 622 | GET /ebanking/scripts/jquery/jquery-ui-1.11.4/jquery-ui.css HTTP/1.1 |
| 81 | 1.634372 | 192.168.1.210 | 176.56.156.22 | HTTP | 603 | GET /ebanking/styles/virtualKeyboard.css HTTP/1.1 |
| 89 | 1.643090 | 192.168.1.210 | 176.56.156.22 | HTTP | 579 | GET /ebanking/scripts/expand.js HTTP/1.1 |
| 107 | 1.646663 | 176.56.156.22 | 192.168.1.210 | HTTP | 217 | HTTP/1.1 304 OK |
| 108 | 1.647375 | 192.168.1.210 | 176.56.156.22 | HTTP | 589 | GET /ebanking/scripts/ebanking_generic.js HTTP/1.1 |
| 110 | 1.647537 | 192.168.1.210 | 176.56.156.22 | HTTP | 593 | GET /ebanking/scripts/jquery/jquery-1.11.3.js HTTP/1.1 |
| 111 | 1.647843 | 192.168.1.210 | 176.56.156.22 | HTTP | 540 | GET /ebanking/dwr/interface/DWRServices.js HTTP/1.1 |
| 112 | 1.647969 | 192.168.1.210 | 176.56.156.22 | HTTP | 607 | GET /ebanking/dwr/engine.js HTTP/1.1 |
| 113 | 1.650300 | 176.56.156.22 | 192.168.1.210 | HTTP | 228 | HTTP/1.1 304 Not Modified |
| 114 | 1.650866 | 192.168.1.210 | 176.56.156.22 | HTTP | 605 | GET /ebanking/dwr/util.js HTTP/1.1 |
| 116 | 1.654181 | 176.56.156.22 | 192.168.1.210 | HTTP | 218 | HTTP/1.1 304 OK |
| 120 | 1.664668 | 176.56.156.22 | 192.168.1.210 | HTTP | 218 | HTTP/1.1 304 OK |
| 121 | 1.668977 | 176.56.156.22 | 192.168.1.210 | HTTP | 228 | HTTP/1.1 304 Not Modified |

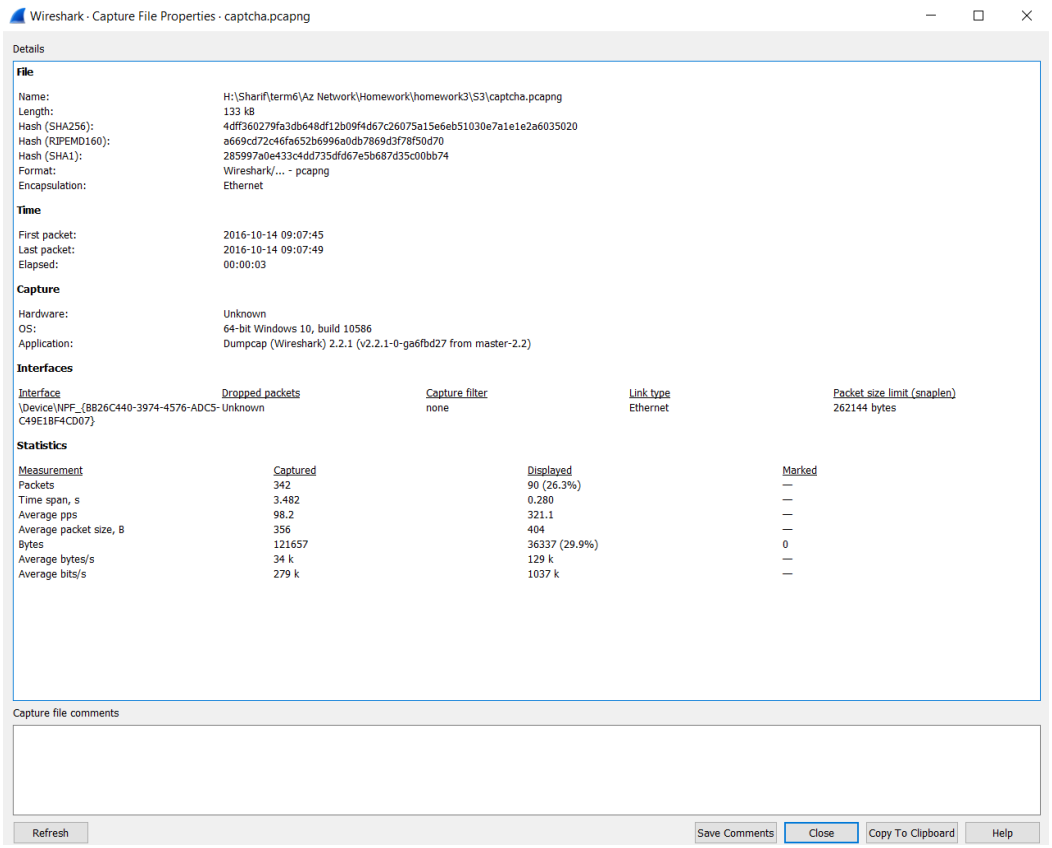


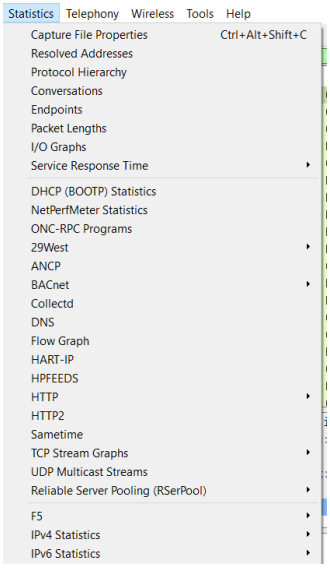

حال با گزینه save عکس داده شده را ذخیره می‌کنیم.

این همان کپچای خواسته‌شده است.✅

## سوالات :

1. مطابق شکل زیر اگر statistics را باز کنیم، می‌توانیم تعداد فیلد انتخاب کنیم.

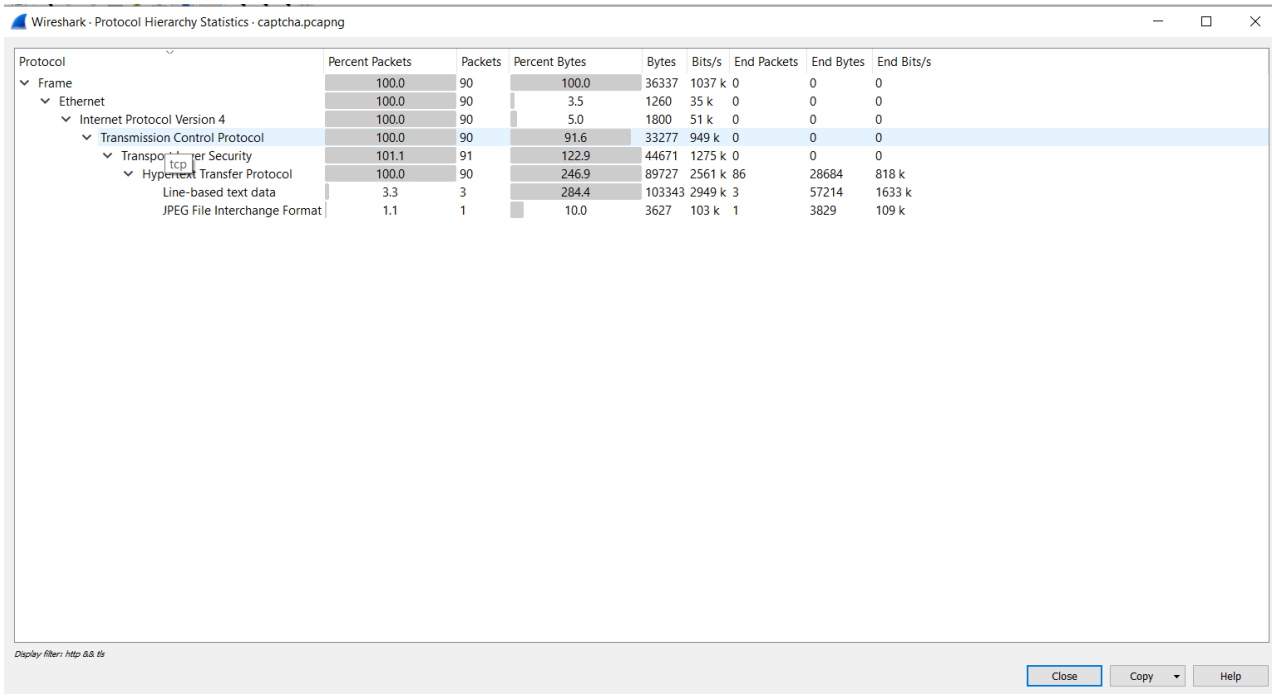



پنجره Capture File Properties را باز می‌کنیم و اطلاعات را طبق شکل بالا بررسی می‌کنیم.

همانطور مشاهده می‌کنیم، در این بسته فرمت کدگذاری فایل مشخص شده که به واسطه آن شاید بتوان برخی فایل‌ها را با تکنیک‌های رمزنگاری، رمزگشایی کرد.

همچنین در پنجره Protocol Hierarchy Statistics مطابق شکل زیر می‌توان اطلاعاتی از پروتکل‌های استفاده شده توسط بسته‌ها بدست آورد.



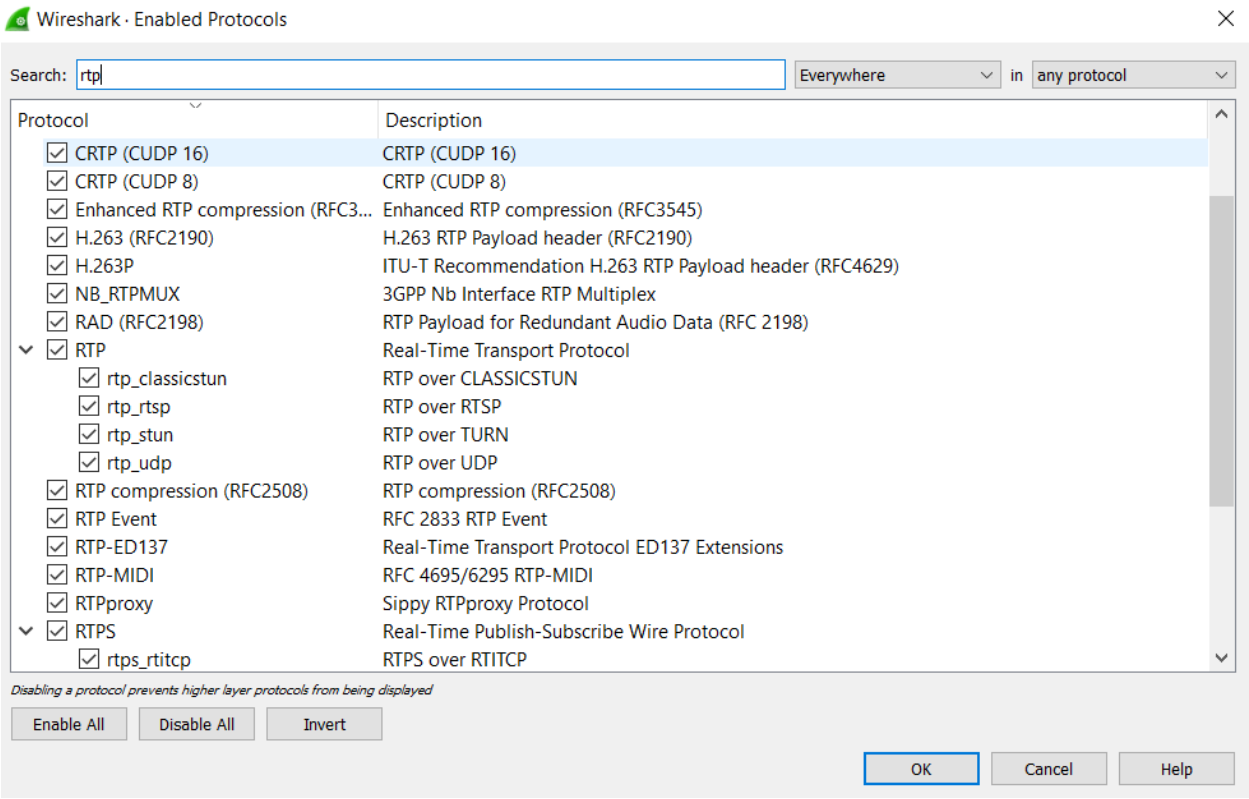

به طور خلاصه، مواردی که در این بخش می‌توان به آنها اشاره کرد، موارد زیر است:

- اطلاعات مختلف برای فایل pcapng مانند زمان، تعداد، سرعت، حجم و ... برای پکت‌ها
- اطلاعات آماری طول پکت‌ها  مانند میانگین، تعداد و درصد در هر بازه عددی و ...
- تفکیک بر اساس پروتکل‌های مختلف و ارائه آماری مانند درصد نسبی، تعداد، حجم و ...
- نمایش اتصالات برقرار شده با تفکیک IP و port مبدا و مقصد با ارائه آماری
- اطلاعات آماری برای پروتکل DNS مانند تعداد هر تایپ DNS، تعداد جواب‌ها، تعداد خطاها و ...

2. پروتکل RTP یک پروتکل بی‌درنگ برای انتقال صدا و تصاویر در شبکه‌های IP است که برای استریم کردن داده استفاده می‌شود.
این پروتکل معمولا با یک پروتکل سیگنال مانند SIP استفاده می‌شود که به منزله شروع استریم داده است.
گاهی اوقات این استریم داده به واسطه UDP یا TCP انجام می‌شود و گاهی نیز

این استریم رمزگذاری شده و با یک لایه ssl منتقل می‌شود.

حال برای فعالسازی و دیدن این پروتکل ابتدا باید به قسمت Analyze و سپس enabled protocols رفت و سپس rtp را برای انواع بسته‌ها فعال کرد.




سپس باید بسته‌های rtp را کپچر کنیم.

نکته این است که در صورتی که بسته با رمزگذاری tls رمزگذاری شده باشد، وایرشارک نمی‌تواند آن را به عنوان rtp تشخیص دهد.

پس از یک trick کوچک استفاده می‌کنیم.

با استفاده از دستورات زیر کلیه sslkey ها را در یک فایل لاگ می‌ریزیم و سپس آن فایل را در preferences به tls می‌دهیم تا دیکود را انجام دهد.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd $HOME\desktop
PS C:\Users\VivoBook\desktop>  SetX SSLKEYLOGFILE "$(get-location)\ssl.log"

SUCCESS: Specified value was saved.
PS C:\Users\VivoBook\desktop> Get-ChildItem ENV: | findstr SSLKEYLOGFILE
SSLKEYLOGFILE                 C:\Users\VivoBook\App Data\ssl-keys.log
PS C:\Users\VivoBook\desktop>
```

حال با باز کردن کروم می‌بینیم که تمامی کلیدهای ssl در یک فایل به اسم ssl.logs در صفحه اصلی ذخیره می‌شوند.

حال پس از دادن فایل کلید لاگ به برنامه wireshark می‌توانیم پکیج‌ها را دیکود کنیم.

حال با فیلتر کردن پکت‌های rtp، می‌توانیم آنها را مشاهده کنیم.

| | | | | | | |
|---|---|---|---|---|---|---|
| 7465 | 106.820443 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 8762 | 127.636863 | 192.168.1.104 | 151.80.120.114 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=63976, Time=984195826[Malformed Packet] |
| 8773 | 127.687964 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 8778 | 127.738790 | 192.168.1.104 | 208.83.20.20 | RTP | 140 | PT=DynamicRTP-Type-108, SSRC=0x1, Seq=24033, Time=2683179623 |
| 9868 | 138.557155 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 12254 | 157.650688 | 192.168.1.104 | 37.235.174.46 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=15794, Time=1661906311, Mark |
| 12260 | 157.660530 | 192.168.1.104 | 151.80.120.114 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=63976, Time=984195826[Malformed Packet] |
| 12265 | 157.697554 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 12318 | 157.791344 | 192.168.1.104 | 208.83.20.20 | RTP | 140 | PT=DynamicRTP-Type-108, SSRC=0x1, Seq=24033, Time=2683179623 |
| 18552 | 338.086710 | 192.168.1.104 | 151.80.120.114 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=63976, Time=984195826[Malformed Packet] |
| 18553 | 338.087392 | 192.168.1.104 | 208.83.20.20 | RTP | 140 | PT=DynamicRTP-Type-108, SSRC=0x1, Seq=24033, Time=2683179623 |
| 18554 | 338.087979 | 192.168.1.104 | 184.105.151.166 | RTP | 140 | PT=ITU-T G.711 PCMA, SSRC=0x1, Seq=57823, Time=2062938, Mark |
| 18615 | 338.697864 | 192.168.1.104 | 61.222.178.254 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=33697, Time=4165944527, Mark |
| 21056 | 397.718321 | 192.168.1.104 | 151.80.120.114 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=63976, Time=984195826[Malformed Packet] |
| 21066 | 397.758467 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 21083 | 397.816464 | 192.168.1.104 | 208.83.20.20 | RTP | 140 | PT=DynamicRTP-Type-108, SSRC=0x1, Seq=24033, Time=2683179623 |
| 23882 | 418.800582 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 23886 | 418.805076 | 192.168.1.104 | 176.56.2.99 | RTP | 140 | PT=16-bit uncompressed audio, stereo, SSRC=0x1, Seq=13067, Time=451398289, Mark |
| 23897 | 418.842220 | 192.168.1.104 | 151.80.120.114 | RTP | 140 | PT=Unassigned, SSRC=0x1, Seq=63976, Time=984195826[Malformed Packet] |

حال از قسمت telephony بالای برنامه wireshark می‌توان پکت‌های rtp را انالیز کرد.

Wireshark · RTP Streams · Wi-Fi

| Source Address | Source Port | Destination Address | Destination Port | SSRC | Start Time | Duration | Payload | Packets | Lost | Min Delta (ms) | Mean Delta (ms) | Max Delta (ms) | Min Jitter | Mean Jitter |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.1.104 | 51984 | 176.56.2.99 | 6969 | 0x1 | 2032.074164 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 59319 | 217.30.10.77 | 6969 | 0x1 | 2000.166032 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 59324 | 176.56.2.99 | 6969 | 0x1 | 2000.115580 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 59311 | 208.83.20.20 | 6969 | 0x1 | 1999.969440 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 54281 | 217.30.10.77 | 6969 | 0x1 | 1999.969157 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 60251 | 217.30.10.77 | 6969 | 0x1 | 1941.384601 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 63108 | 208.83.20.20 | 6969 | 0x1 | 1905.033458 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 63116 | 217.30.10.77 | 6969 | 0x1 | 1904.937359 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 63121 | 176.56.2.99 | 6969 | 0x1 | 1904.919539 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 63114 | 37.235.174.46 | 2710 | 0x1 | 1904.895124 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 62480 | 176.56.2.99 | 6969 | 0x1 | 1904.882781 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 53926 | 208.83.20.20 | 6969 | 0x1 | 1879.006736 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 53939 | 176.56.2.99 | 6969 | 0x1 | 1878.922947 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 53932 | 37.235.174.46 | 2710 | 0x1 | 1878.906811 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 53934 | 217.30.10.77 | 6969 | 0x1 | 1878.904453 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 53918 | 176.56.2.99 | 6969 | 0x1 | 1878.853098 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 58603 | 208.83.20.20 | 6969 | 0x1 | 1815.004995 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 64868 | 176.56.2.99 | 6969 | 0x1 | 1814.862028 | 0.00 | 16-bit audio, stereo | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 64843 | 217.30.10.77 | 6969 | 0x1 | 1803.097013 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 64835 | 208.83.20.20 | 6969 | 0x1 | 1800.955832 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 55017 | 217.30.10.77 | 6969 | 0x1 | 1796.862959 | 0.00 | Unassigned | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 55009 | 208.83.20.20 | 6969 | 0x1 | 1796.438994 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |
| 192.168.1.104 | 55007 | 208.83.20.20 | 6969 | 0x1 | 1796.089097 | 0.00 | RTPType-108 | 1 | 0 (0.0%) | -1.000000 | 0.000000 | 0.000000 | -1.000000 | 0.000000 |

188 streams, 1 selected, 1 total packets. Right-click for more options.

Limit to display filter  Time of Day

Find Reverse | Analyze | Prepare Filter | Play Streams | Copy | Export | Close | Help

# راه‌اندازی DNS Server

برای این کار ابتدا یک فروادر قرار می‌دهیم که ما برای این کار از **خدمات گوگل** استفاده می‌کنیم.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
                8.8.8.8;
                8.8.4.4;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

این کار را در قسمت **/etc/bind/named.conf.options** انجام می‌دهیم.

سپس سرویس بایند را ری استارت می‌کنیم تا تغییرات انجام شود.

حال مطابق مراحل زیر به ترتیب جلو می‌رویم.

```
bigwhoman@bigwhoman-pp /e/bind> cat 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 NetLab2.edu {
        type master;
        file "/etc/bind/db.NetLab2.edu";
};

zone "1.0.0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.reverse.NetLab2.edu";
};
```

```
bigwhoman@bigwhoman-pp /e/bind> cat /etc/bind/db.NetLab2.edu
$TTL    604800
@       IN      SOA     ns1.NetLab2.edu. admin.NetLab2.edu. (
                              10         ; Serial
                          604800         ; Refresh
                           86400         ; Retry
                         2419200         ; Expire
                          604800 )       ; Negative Cache TTL
@       IN      NS      ns1.NetLab2.edu.
ns1     IN      A       127.0.0.1

g1      IN      CNAME   group1
group1  IN      A       127.0.0.2

g2      IN      CNAME   group2
group2  IN      A       127.0.0.3
```

```
bigwhoman@bigwhoman-pp /e/bind> cat db.reverse.NetLab2.edu
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.NetLab2.edu. admin.NetLab2.edu. (
                              3         ; Serial
                          604800         ; Refresh
                           86400         ; Retry
                         2419200         ; Expire
                          604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.NetLab2.edu.

1.0.0   IN      PTR     ns1.NetLab2.edu.
2.0.0   IN      PTR     group1.NetLab2.edu.
3.0.0   IN      PTR     group2.NetLab2.edu.
```

```
bigwhoman@bigwhoman-pp /e/bind> sudo named-checkzone 1.0.0.in-addr.arpa db.reverse.NetLab2.edu
zone 1.0.0.in-addr.arpa/IN: loaded serial 3
OK
```

```
bigwhoman@bigwhoman-pp /e/bind> sudo named-checkzone NetLab2.edu db.NetLab2.edu
zone NetLab2.edu/IN: loaded serial 8
OK
```

```
bigwhoman@bigwhoman-pp /e/bind> sudo service bind9 restart
bigwhoman@bigwhoman-pp /e/bind> sudo service bind9 status
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-03-29 16:55:51 +0330; 3s ago
       Docs: man:named(8)
    Process: 44782 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 44783 (named)
      Tasks: 14 (limit: 14070)
     Memory: 9.7M
        CPU: 32ms
     CGroup: /system.slice/named.service
             └─44783 /usr/sbin/named -u bind

16:55:51 29 ماس bigwhoman-pp named[44783]: managed-keys-zone: loaded serial 13
16:55:51 29 ماس bigwhoman-pp named[44783]: zone 1.0.0.in-addr.arpa/IN: loaded serial 3
16:55:51 29 ماس bigwhoman-pp named[44783]: zone 0.in-addr.arpa/IN: loaded serial 1
16:55:51 29 ماس bigwhoman-pp named[44783]: zone 255.in-addr.arpa/IN: loaded serial 1
16:55:51 29 ماس bigwhoman-pp named[44783]: zone 127.in-addr.arpa/IN: loaded serial 1
16:55:51 29 ماس bigwhoman-pp named[44783]: zone localhost/IN: loaded serial 2
16:55:51 29 ماس bigwhoman-pp named[44783]: zone NetLab2.edu/IN: loaded serial 8
16:55:51 29 ماس bigwhoman-pp named[44783]: all zones loaded
16:55:51 29 ماس bigwhoman-pp named[44783]: running
16:55:51 29 ماس bigwhoman-pp systemd[1]: Started BIND Domain Name Server.
bigwhoman@bigwhoman-pp /e/bind> host ns1.NetLab2.edu
```

```
bigwhoman@bigwhoman-pp /e/bind> host ns1.NetLab2.edu
ns1.NetLab2.edu has address 127.0.0.1
bigwhoman@bigwhoman-pp /e/bind> host group1.NetLab2.edu
group1.NetLab2.edu has address 127.0.0.2
bigwhoman@bigwhoman-pp /e/bind> host group2.NetLab2.edu
group2.NetLab2.edu has address 127.0.0.3
```

```
bigwhoman@bigwhoman-pp /e/bind> host g1.NetLab2.edu
g1.NetLab2.edu is an alias for group1.NetLab2.edu.
group1.NetLab2.edu has address 127.0.0.2
bigwhoman@bigwhoman-pp /e/bind> host g2.NetLab2.edu
g2.NetLab2.edu is an alias for group2.NetLab2.edu.
group2.NetLab2.edu has address 127.0.0.3
```

```
bigwhoman@bigwhoman-pp /e/bind> ping google.com
PING google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=51 time=115 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=51 time=73.1 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=51 time=95.3 ms
```

```
bigwhoman@bigwhoman-pp /e/bind> dig google.com

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31814
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2a4ec7b907c5ff850100000064243cc79f321e86c656a4a7 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             56      IN      A       216.239.38.120

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Mar 29 16:57:35 +0330 2023
;; MSG SIZE  rcvd: 83
```

```
bigwhoman@bigwhoman-pp /e/bind> ping group1.NetLab2.edu
PING group1.NetLab2.edu (127.0.0.2) 56(84) bytes of data.
64 bytes from 127.0.0.2 (127.0.0.2): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 127.0.0.2 (127.0.0.2): icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 127.0.0.2 (127.0.0.2): icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 127.0.0.2 (127.0.0.2): icmp_seq=4 ttl=64 time=0.048 ms
^C
--- group1.NetLab2.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.029/0.043/0.048/0.008 ms
bigwhoman@bigwhoman-pp /e/bind> ping group2.NetLab2.edu
PING group2.NetLab2.edu (127.0.0.3) 56(84) bytes of data.
64 bytes from 127.0.0.3 (127.0.0.3): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from 127.0.0.3 (127.0.0.3): icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 127.0.0.3 (127.0.0.3): icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 127.0.0.3 (127.0.0.3): icmp_seq=4 ttl=64 time=0.048 ms
64 bytes from 127.0.0.3 (127.0.0.3): icmp_seq=5 ttl=64 time=0.045 ms
^C
--- group2.NetLab2.edu ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4100ms
rtt min/avg/max/mdev = 0.029/0.043/0.050/0.007 ms
```

## سوالات :

1. مطابق زیر به سه آدرس درخواست می‌فرستیم و جواب‌ها را بررسی می‌کنیم.

مشاهده می‌کنیم که درخواست ما برای آدرس ۱۲۷.۰.۰.۱ که همان آدرس دی ان اس سرور لوکال است فرستاده می‌شود و سپس برای **۸.۸.۴.۴ فوروارد** می‌شود.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 867 | 37.443584283 | 127.0.0.1 | 127.0.0.1 | DNS | 95 | Standard query 0xcca5 A google.com OPT |
| 868 | 37.443748559 | 192.168.2.125 | 8.8.4.4 | DNS | 72 | Standard query 0x2348 A google.com |
| 869 | 37.485810707 | 8.8.4.4 | 192.168.2.125 | DNS | 88 | Standard query response 0x2348 A google.com A 216.239.38.120 |
| 870 | 37.485942052 | 8.8.4.4 | 192.168.2.125 | DNS | 88 | Standard query response 0x2348 A google.com A 216.239.38.120 |
| 871 | 37.486005152 | 127.0.0.1 | 127.0.0.1 | DNS | 127 | Standard query response 0xcca5 A google.com A 216.239.38.120 OPT |

```
bigwhoman@bigwhoman-pp /v/log> nslookup gamefa.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   gamefa.com
Address: 79.127.127.16
```

| | | | | | | |
|---|---|---|---|---|---|---|
| 216 | 20.811072107 | 127.0.0.1 | 127.0.0.1 | DNS | 72 | Standard query 0x6a47 A gamefa.com |
| 217 | 20.811256365 | 192.168.2.125 | 8.8.4.4 | DNS | 72 | Standard query 0xe9bd A gamefa.com |
| 218 | 21.000232175 | 8.8.4.4 | 192.168.2.125 | DNS | 88 | Standard query response 0xe9bd A gamefa.com A 79.127.127.16 |
| 219 | 21.000660156 | 127.0.0.1 | 127.0.0.1 | DNS | 88 | Standard query response 0x6a47 A gamefa.com A 79.127.127.16 |

```
bigwhoman@bigwhoman-pp /v/log> dig g1.NetLab2.edu

; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> g1.NetLab2.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45318
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a3b76ff57d951aef0100000064246d63b22a5009dcf5b366 (good)
;; QUESTION SECTION:
;g1.NetLab2.edu.                        IN      A

;; ANSWER SECTION:
g1.NetLab2.edu.         604800  IN      CNAME   group1.NetLab2.edu.
group1.NetLab2.edu.     604800  IN      A       127.0.0.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Mar 29 20:24:59 +0330 2023
;; MSG SIZE  rcvd: 108
```

| | | | | | | |
|---|---|---|---|---|---|---|
| 10163 | 483.985809487 | 127.0.0.1 | 127.0.0.1 | DNS | 99 | Standard query 0xb106 A g1.NetLab2.edu OPT |
| 10164 | 483.985931167 | 127.0.0.1 | 127.0.0.1 | DNS | 152 | Standard query response 0xb106 A g1.NetLab2.edu CNAME group1.NetLab2.edu A 127.0.0.2 OPT |

2. مطابق شکل‌های زیر دو درخواست برای ریزالو کردن سایت , gamefa.com
google.com به شکل A record هستند و نیز درخواست آخر که همان
g1.NetLab2.edu است به شکل CNAME است.

```
▾ Queries
  ▾ gamefa.com: type A, class IN
      Name: gamefa.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 219]
```

```
▾ Queries
  ▾ google.com: type A, class IN
      Name: google.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▾ Answers
  ▾ google.com: type A, class IN, addr 216.239.38.120
      Name: google.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 4
      Address: 216.239.38.120
```

```
▾ Queries
  ▾ g1.NetLab2.edu: type A, class IN
      Name: g1.NetLab2.edu
      [Name Length: 14]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▾ Answers
  ▾ g1.NetLab2.edu: type CNAME, class IN, cname group1.NetLab2.edu
      Name: g1.NetLab2.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 604800 (7 days)
      Data length: 9
      CNAME: group1.NetLab2.edu
  ▾ group1.NetLab2.edu: type A, class IN, addr 127.0.0.2
      Name: group1.NetLab2.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 604800 (7 days)
      Data length: 4
      Address: 127.0.0.2
```