آزمایش شماره ۳

آز شبکه ـ دکتر بردیا صفایی

دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف

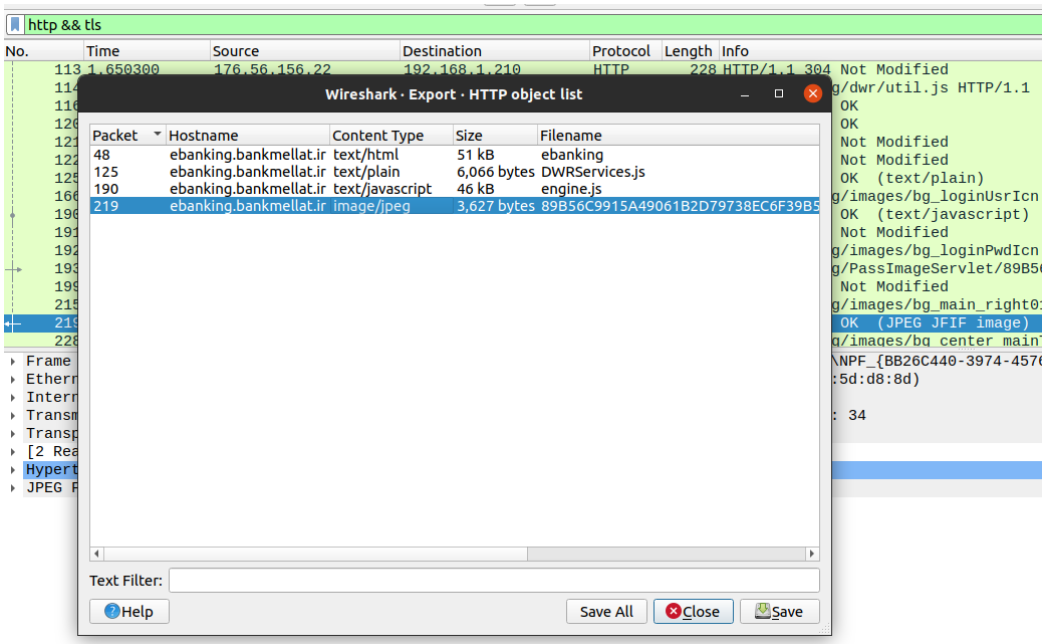
نیم‌سال اول ۰۱ـ۰۲

مهرشاد میرمحمدی ـ ۹۸۱۰۹۶۳۴
پرهام صارمی ـ ۹۷۱۰۱۹۵۹
محمدرضا مفیضی ـ ۹۸۱۰۶۰۵۹

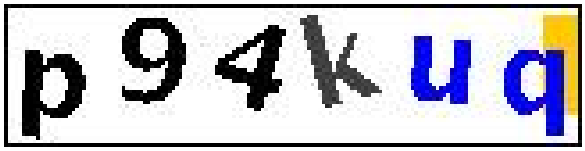
۱ wireshark

۱.۱ بدست‌آوردن captcha

همانند دستور عمل می‌کنیم، با این تفاوت که به جای استفاده ازهمانند دستور عمل می‌کنیم، با این تفاوت که به جای استفاده از SSL ، از TLS استفاده می‌کنیم. دلیل آن هم این است که SSL منسوخ شده و TLS جای آن را گرفته است. همچنین این پروتکل در ورژن wireshark مورد استفاده موجود نبود. لیست فایل‌های استخراج شده و یcaptcha بدست‌آمده را می‌توان در تصاویر ۱ و ۲ دید.



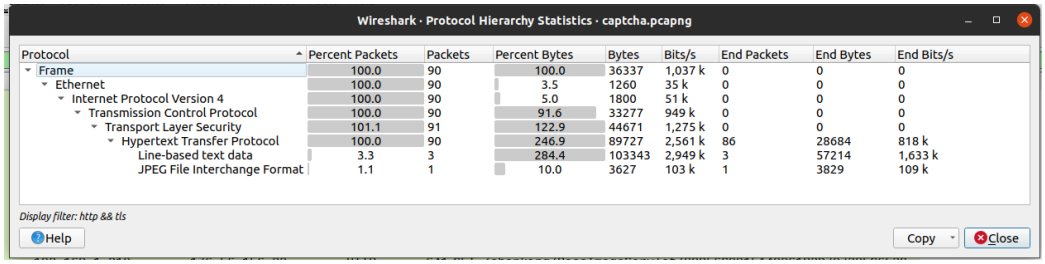
شکل ۱ : پنجره‌ی ذخیره‌سازی فایل‌های بدست‌آمده.



شکل ۲ : عکس بدست‌آمده.

۲.۱ سوال‌ها

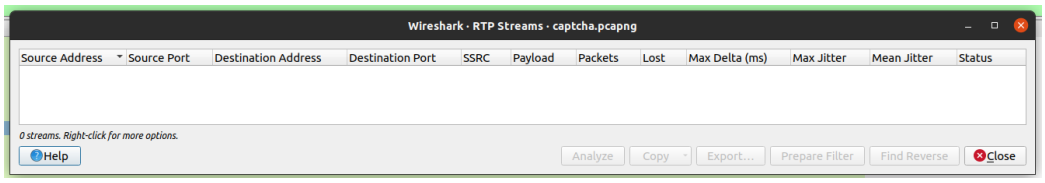
۱. این اطلاعات و آماره‌ها را می‌توان از طریق منوی statistics موجود در wireshark بدست آورد. برای مثال با استفاده از بخش سلسله مراتب پروتکل‌ها می‌توان دید پروتکل‌های استفاده شده کدام‌ها هستند، از هر کدام چند پکت موجود است و چند درصد از پکت‌ها و بایت‌ها برای آن بوده است. تصویر ۳ نمونه خروجی این ابزار است. همچنین با استفاده از باقی ابزارها می‌توان اطلاعات دیگری همانند طول بسته‌ها، ترافیک و تعداد بسته‌های بین بخش‌های مختلف شبکه، زمان بین پاسخ‌ها و ... بدست‌آورد.



شکل ۳: Hierarchy Protocols < statistics

۲. پروتکل RTP یک پروتکل بیدرنگ برای انتقال صدا و تصویر در شبکه‌ها با بستر IP است. این پروتکل معمولا بر پایه‌ی UDP است و برای streaming استفاده می‌شود. همچنین معمولا برای کنترل ترتیب رسیدن بسته‌ها، از پرتوکل RTCP هم به همراه آن استفاده می‌شود.

در wireshark می‌توان با رفتن به Telephony سپس RTP و سپس streams RTP اطلاعات مربوط به آن را یافت. اطلاعاتی مانند آدرس و پورت مبدا و مقصد، میانگین و حداکثر jitter ، گمشدگی و ... که در تصویر ۴ هم می‌توان دید. همچنین امکان ضبط و بخش محتوا به صورت مستقیم هم موجود است.



شکل ۴: Streams RTP < RTP < Telephony

۲ DNS

ابتدا bind۹ را همانند تصویر ۵ نصب می‌کنیم. ما از ubuntu 20.04 استفاده می‌کنیم.

مطابق شکل ۶ یک منطقه با عنوان NetLab8.edu ایجاد می‌کنیم. (عدد ۸ شماره‌ی گروه است.)

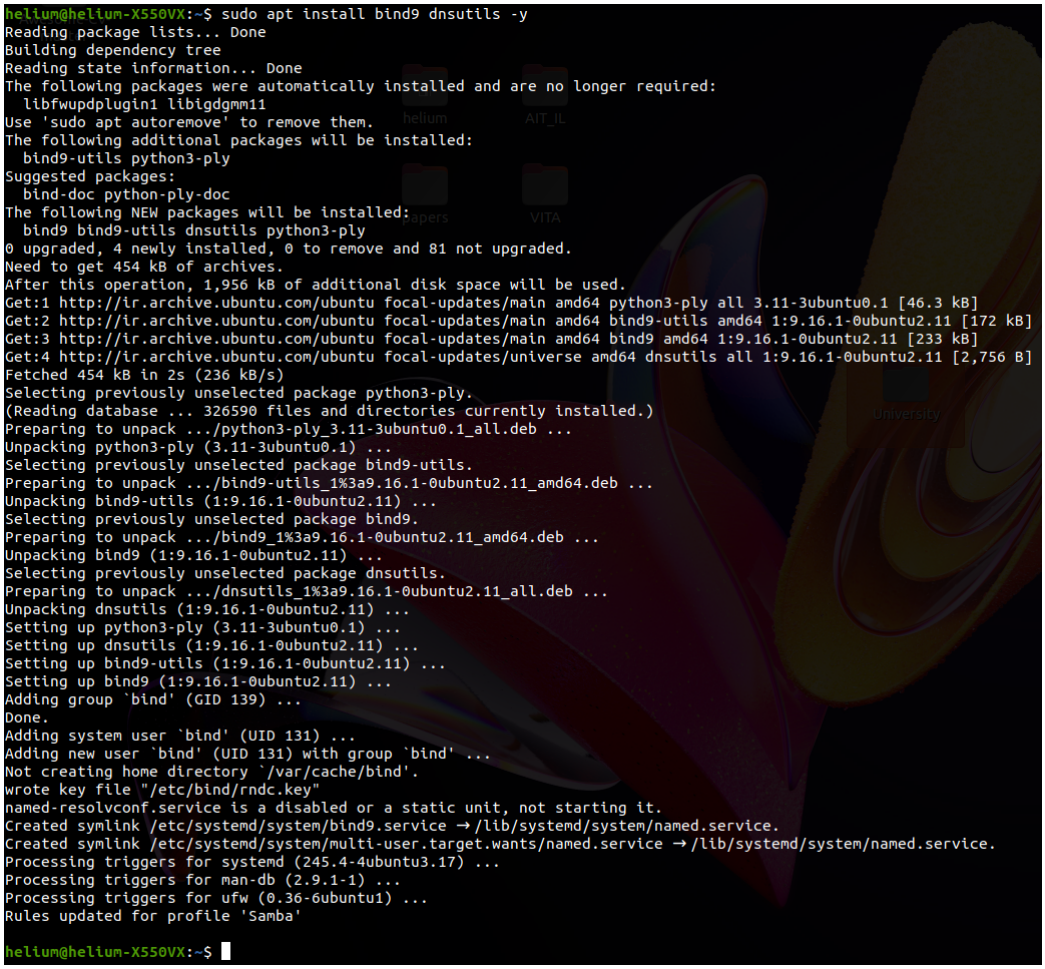
فایل /etc/bind/db.NetLab8.edu مطابق تصویر ۷ پر می‌کنیم. همانطور که در تصویر مشخص است یک nameserver با نام ns.NetLab8.edu و ip با مقدار ۱۹۲.۱۶۸.۸.۱ ایجاد می‌کنیم. به دامنه‌ی سرور آدرس ۱۹۲.۱۶۸.۸.۲ اختصاص می‌دهیم. دو زیر دامنه‌ی group1.NetLab8.edu و group2.NetLab8.edu را به ترتیب در ip های ۱۹۲.۱۶۸.۸.۳ و ۱۹۲.۱۶۸.۸.۴ و با نام‌های مستعار cNameGroup1.NetLab8.edu و cNameGroup2.NetLab8.edu تعریف می‌کنیم.

مطابق تصویر ۸ تنظیمات رکوردهای معکوس را هم در فایل /etc/bind/db.192.168.8 قرار می‌دهیم.

فایل /etc/resolvconf/resolv.conf.d/head را مطابق تصویر ۹ پر می‌کنیم.

سپس دستورهای زیر را به ترتیب اجرا می‌کنیم تا bind9 مجددا راه‌اندازی شده و آدرس سرور ما قبل از همه‌ی سرویس‌دهنده‌های مورد اعتماد سیستم قرار بگیرد. سپس با استفاده با دستور nslookup از درستی کارکرد سرور DNS اطمینان حاصل می‌کنیم. (مطابق تصاویر ۱۰ و ۱۱)

```
sudo systemctl restart bind9
sudo named-checkconf
sudo resolvconf -u
```



شکل ۵:

۱.۲ سوالات

۱. اطلاعات پکت‌های DNS رد و بدل شده برای بدست آوردن ip متعلق به group2.NetLab8.edu و نام متعلق به آدرس ۱۹۲.۱۶۸.۸.۳ را با استفاده از وایرشارک capture می‌کنیم. در تصویر ۱۲ و ۱۳ پرس و جو و پاسخ سرور را به ترتیب مشاهده می‌کنیم.

۲. همانطور که در تصاویر هم می‌توانیم ببینیم، نوع پرس و جوی اول از نوع A و نوع پرس و جوی دوم از نوع PTR است.

etc > bind > named.conf.local

```
1   //
2   // Do any local configuration here
3   //
4
5   // Consider adding the 1918 zones here, if they are not us
6   // organization
7   //include "/etc/bind/zones.rfc1918";
8
9   zone "NetLab8.edu" {
10          type master;
11          file "/etc/bind/db.NetLab8.edu";
12  };
13
14  zone "8.168.192.in-addr.arpa" {
15          type master;
16          file "/etc/bind/db.192.168.8";
17  };
```

شکل ۶:

etc > bind > db.NetLab8.edu

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA ns.NetLab8.edu. root.NetLab8.edu. (
                  3     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@   IN  NS  ns.NetLab8.edu.
ns  IN  A   192.168.8.1
@   IN  A   192.168.8.2

group1  IN  A   192.168.8.3
cNameGroup1 IN  CNAME   group1

group2  IN  A   192.168.8.4
cNameGroup2 IN  CNAME   group2

```

شکل ۷:

```
etc > bind > ≡ db.192.168.8
1   ;
2   ; BIND data file for local loopback interface
3   ;
4   $TTL    604800
5   @   IN  SOA ns.NetLab8.edu. root.NetLab8.edu. (
6                   2     ; Serial
7                604800     ; Refresh
8                 86400     ; Retry
9                2419200     ; Expire
10               604800 )   ; Negative Cache TTL
11  ;
12  @   IN  NS  ns.NetLab8.edu.
13  1   IN  PTR ns.NetLab8.edu.
14  2   IN  PTR NetLab8.edu.
15
16  3   IN  PTR group1.NetLab8.edu.
17  4   IN  PTR group2.NetLab8.edu.
18
```

شکل ۸:

```
etc > resolvconf > resolv.conf.d > ≡ head
1   # Dynamic resolv.conf(5) file for glibc resolver(3) genera
2   #     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL B
3   # 127.0.0.53 is the systemd-resolved stub resolver.
4   # run "systemd-resolve --status" to see details about the
5
6   search NetLab8.edu
7   nameserver 127.0.0.1
8
```

شکل ۹:

```
helium@helium-X550VX:~$ nslookup NetLab8.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   NetLab8.edu
Address: 192.168.8.2

helium@helium-X550VX:~$ nslookup ns.NetLab8.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   ns.NetLab8.edu
Address: 192.168.8.1

helium@helium-X550VX:~$ nslookup group1.NetLab8.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   group1.NetLab8.edu
Address: 192.168.8.3

helium@helium-X550VX:~$ nslookup group2.NetLab8.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   group2.NetLab8.edu
Address: 192.168.8.4

helium@helium-X550VX:~$ nslookup cNamegroup1.NetLab8.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

cNameGroup1.NetLab8.edu canonical name = group1.NetLab8.edu.
Name:   group1.NetLab8.edu
Address: 192.168.8.3

helium@helium-X550VX:~$ nslookup cNamegroup2.NetLab8.edu
Server:         127.0.0.1
Address:        127.0.0.1#53

cNameGroup2.NetLab8.edu canonical name = group2.NetLab8.edu.
Name:   group2.NetLab8.edu
Address: 192.168.8.4
```

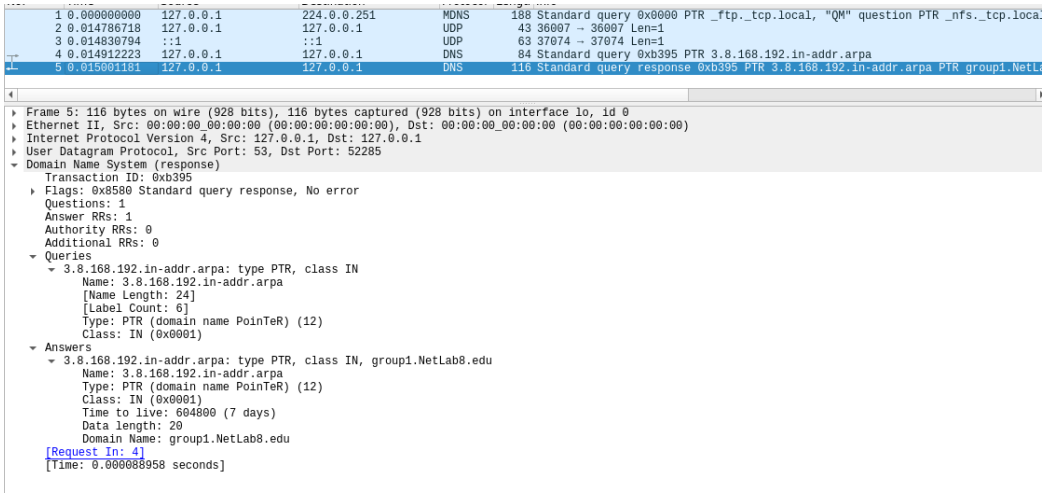
شکل ۱۰:

```
helium@helium-X550VX:~$ nslookup 192.168.8.1
1.8.168.192.in-addr.arpa        name = ns.NetLab8.edu.

helium@helium-X550VX:~$ nslookup 192.168.8.2
2.8.168.192.in-addr.arpa        name = NetLab8.edu.

helium@helium-X550VX:~$ nslookup 192.168.8.3
3.8.168.192.in-addr.arpa        name = group1.NetLab8.edu.

helium@helium-X550VX:~$ nslookup 192.168.8.4
4.8.168.192.in-addr.arpa        name = group2.NetLab8.edu.
```

شکل ۱۱:

```
    1 0.000000000   127.0.0.1           127.0.0.1           UDP       43 55906 → 55906 Len=1
    2 0.000098636   ::1                 ::1                 UDP       63 43383 → 43383 Len=1
    3 0.000257602   127.0.0.1           127.0.0.1           DNS       78 Standard query 0x28c8 A group2.NetLab8.edu
    4 0.000441480   127.0.0.1           127.0.0.1           DNS       94 Standard query response 0x28c8 A group2.NetLab8.edu A 192.168.8.4
    5 0.001027544   127.0.0.1           127.0.0.1           DNS       78 Standard query 0x4c0e AAAA group2.NetLab8.edu
    6 0.001108856   127.0.0.1           127.0.0.1           DNS      122 Standard query response 0x4c0e AAAA group2.NetLab8.edu SOA ns.NetLab8.edu
▸ Frame 4: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface lo, id 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 55746
▾ Domain Name System (response)
    Transaction ID: 0x28c8
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ group2.NetLab8.edu: type A, class IN
        Name: group2.NetLab8.edu
        [Name Length: 18]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ group2.NetLab8.edu: type A, class IN, addr 192.168.8.4
        Name: group2.NetLab8.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 604800 (7 days)
        Data length: 4
        Address: 192.168.8.4
    [Request In: 3]
    [Time: 0.000183878 seconds]
```

شکل ۱۲:


1 0.000000000 127.0.0.1 224.0.0.251 MDNS 188 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local
2 0.014786718 127.0.0.1 127.0.0.1 UDP 43 36007 → 36007 Len=1
3 0.014830794 ::1 ::1 UDP 63 37074 → 37074 Len=1
4 0.014912223 127.0.0.1 127.0.0.1 DNS 84 Standard query 0xb395 PTR 3.8.168.192.in-addr.arpa
5 0.015001181 127.0.0.1 127.0.0.1 DNS 116 Standard query response 0xb395 PTR 3.8.168.192.in-addr.arpa PTR group1.NetLa
Frame 5: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 53, Dst Port: 52285
Domain Name System (response)
Transaction ID: 0xb395
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
3.8.168.192.in-addr.arpa: type PTR, class IN
Name: 3.8.168.192.in-addr.arpa
[Name Length: 24]
[Label Count: 6]
Type: PTR (domain name PoinTeR) (12)
Class: IN (0x0001)
Answers
3.8.168.192.in-addr.arpa: type PTR, class IN, group1.NetLab8.edu
Name: 3.8.168.192.in-addr.arpa
Type: PTR (domain name PoinTeR) (12)
Class: IN (0x0001)
Time to live: 604800 (7 days)
Data length: 20
Domain Name: group1.NetLab8.edu
[Request In: 4]
[Time: 0.000088958 seconds]

شکل ۱۳: