شبکه‌های کامپیوتری

تمرین دوم

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

نیم سال دوم ۰۰-۹۹

استاد:

جناب آقای دکتر جعفری

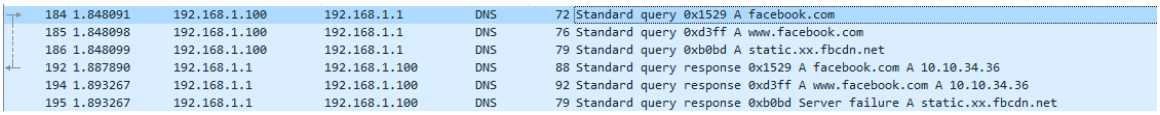
نام و نام خانوادگی:

امیرمهدی نامجو - ۹۷۱۰۷۲۱۲

۱ سوال اول

توجه: امکان زوم بر روی تمامی تصاویری که در متن قرار دارند وجود دارد.

۱. وضعیت درخواست‌های DNS رد و بدل شده برای فیسبوک به صورت زیر است:

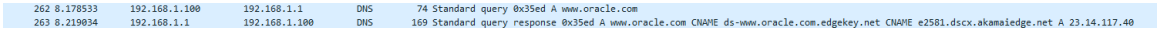


سه درخواست اول از کامپیوتر من به روتر رفته‌اند و سه مورد بعدی جواب‌هایی هستند که از روتر به کامپیوتر من برگشته اند. مشاهده می‌کنیم آدرس آی‌پی که برای فیسبوک برگشته است 10.10.34.36 است.

این آدرس آی‌پی جزو دسته آی‌پی‌های رزرو شده است که بین 10.0.0.0 تا 10.255.255.255 قرار دارد. این آدرس آی‌پی‌ها مربوط به شبکه‌های خصوصی هستند و عملا به سایت خاصی در اینترنت نگاشت نشده‌اند. این یعنی DNS سرور، آدرسی را برای سایت Facebook برگردانده که عملا مربوط به شبکه عمومی اینترنت نمی‌شود و یک آدرس در شبکه خصوصی است که عملا در کامپیوتر من وجود نداشته و نتیجتا کروم با خطای This site can’t be reached و ERR_CONNECTION_TIMED_OUT متوقف می‌شود.

با بررسی تنظیمات مودم متوجه شدم که DNS-Server پیش‌فرض آن به صورت 46.224.1.220 است که با IpLookup کردن آن، متوجه می‌شویم که این آی‌پی متعلق به ns5.hiweb.ir یعنی Nameserver «های‌وب» در ایران است و منطقی است که فیلترینگ روی این Nameserver داخلی اعمال شده باشد و در نتیجه DNS به آن نتیجه نامعتبری برای facebook.com که یک سایت فیلتر شده است برگرداند.

۲. وضعیت درخواست DNS برای سایت اوراکل به صورت زیر است:



وضعیت خروجی برگدانده شده برای آن به صورت زیر است:

```
Answers
www.oracle.com: type CNAME, class IN,
 cname ds-www.oracle.com.edgekey.net
Name: www.oracle.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 497 (8 minutes, 17 seconds)
Data length: 31
```

```
CNAME: ds-www.oracle.com.edgekey.net
ds-www.oracle.com.edgekey.net: type CNAME, class IN,
 cname e2581.dscx.akamaiedge.net
Name: ds-www.oracle.com.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 451 (7 minutes, 31 seconds)
Data length: 24
CNAME: e2581.dscx.akamaiedge.net
e2581.dscx.akamaiedge.net: type A, class IN, addr 23.14.117.40
Name: e2581.dscx.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 497 (8 minutes, 17 seconds)
Data length: 4
Address: 23.14.117.40
```

جواب اول مشخص می‌کند که `www.oracle.com` در اصل یک Alias برای یک آدرس دیگر است.

جواب دوم مشخص می‌کند که آدرس مشخص شده بعدی یعنی

`ds-www.oracle.com.edgekey.net`

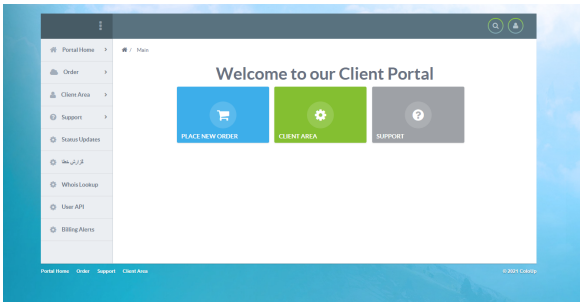
هم یک Alias برای آدرس دیگری است. آدرس نهایی یعنی `e2581.dscx.akamaiedge.net` به یک آدرس آی‌پی واقعی مپ شده است. این آدرس ای‌پی یعنی `23.14.117.40` مربوط به یکی از CDN های شرکت Akamai است. این CDN در ترکیه واقع شده است و براساس موقعیت مکانی من که ایران بوده، نزدیک‌ترین CDN تشخیص داده شده مربوط به کشور ترکیه بوده است. با این وجود در نهایت شاهد این هستیم که سایت Oracle باز نمی‌شود و با خطاهای `This site can’t be reached` و `ERR_CONNECTION_TIMED_OUT` مواجه می‌شویم. این خطاها این بار به خاطر فیلترینگ نیستند بلکه به خاطر تحریم است.

۳. پیش از بررس نتایج باید بررسی کنیم که آی‌پی آدرس DNS-Server های شکن متعلق به کجاست. در سایت دو آی‌پی آدرس قرار گرفته است. اولین مورد `178.22.122.100` است که متعلق به شرکت آسیاتک (Asiatech Data Transmission company) بوده و دومین آی‌پی `185.51.200.2` است که متعلق به شرکت مهندسی صفرویک پرداز (Sefroyek Pardaz Engineering Co. LTD) است.

با انجام تنظیمات مربوطه و وارد کردن آدرس Oracle داریم:

```
489 5.153691    192.168.1.100   178.22.122.100  DNS      74 Standard query 0xa2f2 A www.oracle.com
492 5.221112    192.168.1.100   185.51.200.2    DNS      74 Standard query 0xa2f2 A www.oracle.com
495 5.273204    178.22.122.100  192.168.1.100   DNS     117 Standard query response 0xa2f2 A www.oracle.com CNAME us1.shecan.ir A 162.223.88.52
500 5.276747    185.51.200.2    192.168.1.100   DNS     117 Standard query response 0xa2f2 A www.oracle.com CNAME us1.shecan.ir A 162.223.88.52
635 6.329435    192.168.1.100   178.22.122.100  DNS      79 Standard query 0x2de7 A c.oracleinfinity.io
639 6.395303    192.168.1.100   185.51.200.2    DNS      79 Standard query 0x2de7 A c.oracleinfinity.io
650 6.560923    178.22.122.100  192.168.1.100   DNS     174 Standard query response 0x2de7 A c.oracleinfinity.io CNAME c.oracleinfinity.io.edgekey.net CNAME e11123.g.akamaiedge.net A 95.101.18.83
672 6.787557    185.51.200.2    192.168.1.100   DNS     174 Standard query response 0x2de7 A c.oracleinfinity.io CNAME c.oracleinfinity.io.edgekey.net CNAME e11123.g.akamaiedge.net A 92.123.210.100
755 7.048241    192.168.1.100   178.22.122.100  DNS      73 Standard query 0x70f6 A go.oracle.com
763 7.087405    178.22.122.100  192.168.1.100   DNS     116 Standard query response 0x70f6 A go.oracle.com CNAME us1.shecan.ir A 162.223.88.52
```

همان طور که در تصویر مشخص است در نتیجه درخواست آدرس www.oracle.com خروجی به این صورت بوده که این آدرس Alias ای برای آدرس us1.shecan.ir است و آدرس آی‌پی 162.223.88.52 گزارش شده است. این آدرس آی‌پی در آمریکا قرار داشته و متعلق به شرکتی به اسم ColoUp است. با مراجعه به سایت این شرکت می‌توان مشاهده کرد که این شرکت مرتبط به خدمات شبکه است و البته بخش گزارش خطا به زبان فارسی هم دارد در نتیجه می‌توان به این نتیجه رسید که با شکن در ارتباط است.

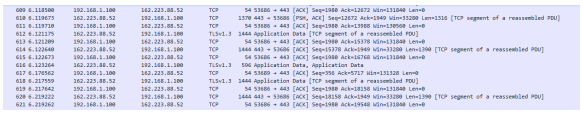


خروجی برگردانده شده به صورت زیر است:

```
Answers
www.oracle.com: type CNAME, class IN, cname us1.shecan.ir
Name: www.oracle.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 118 (1 minute, 58 seconds)
Data length: 15
CNAME: us1.shecan.ir
us1.shecan.ir: type A, class IN, addr 162.223.88.52
Name: us1.shecan.ir
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 214 (3 minutes, 34 seconds)
Data length: 4
Address: 162.223.88.52
```

سایر موارد مربوط به Oracle که مشاهده می‌شود، مربوط به CDN ها و موارد متفرقه دیگری هستند که تحریم نبوده و همان IP اصلی آن ها برگردانده شده است. البته go.oracle.com هم تحریم است و برای آن هم آدرس مربوط به us1.shecan.ir برگردانده شده است.

بدین ترتیب به نظر می‌رسد که درخواست‌هایی که ما برای سایت Oracle می‌فرستیم به جای این که مستقیما به سایت Oracle برود، به سایت واسطه‌ای که آدرس آن us1.shecan.ir است می‌رود و سپس از طریق این سایت به Oracle منتقل شده و جواب‌ها هم از طریق همین سایت با آی‌پی 162.223.88.52 برای ما بر می‌گردد:

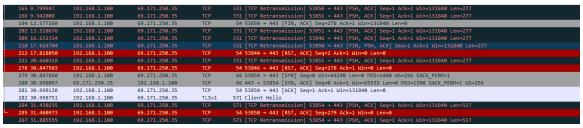


از آن‌جایی که این آی‌پی در آمریکا قرار دارد و درخواست‌های ما از طریق آن به Oracle منتقل می‌شود، Oracle تحریم را اعمال نکرده و اطلاعات را به سرورهای شکن فرستاده و از آن طریق پاسخ مربوطه به ما بر می‌گردد.

در مورد مواردی که تحریم نیستند، آدرس ای‌پی تغییری نمی‌کند و در این زمینه شکن تغییری در روند کار ایجاد نکرده و مانند یک DNS-Server معمولی عمل می‌کند.

نتایجی که برای فیسبوک بر می‌گردد به صورت زیر است:

آی‌پی‌هایی که با آدرس‌های 69.171.250.35 و 157.240.194.35 برگردانده می‌شوند، هر دو واقعا متعلق به فیسبوک هستند. اما با این حال اگر پکت‌های TCP جا به جا شده به این IP را مشاهده کنیم وضعیت زیر را می‌بینیم:



مشاهده می‌شود که اکثر موارد به رنگ سیاه یا قرمز هستند. سیاه با حروف قرمز به معنی BAD TCP و قرمز با حروف زرد به معنی TCP RST است. تقریبا هیچ‌کدام از پکت‌های ارسالی ما به درستی به فیسبوک منتقل نشده‌اند. این بدین معنی است که فیلترینگ اعمال شده برای فیسبوک تنها در لایه DNS نیست. بلکه فیلترینگ‌های دیگری هم اعمال شده است که پکت‌ها را بعد از رسیدن به ISPهای داخلی، با توجه به آدرس آن که مربوط به فیسبوک است و جزو سایت‌های فیلتر شده است، Drop می‌کند تا به فیسبوک نرسند.

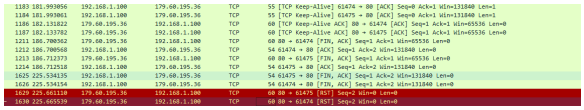
در این مورد Shecan هم نقش خاصی ایفا نکرده و صرفا آدرس واقعی سایت `www.facebook.com` را به ما برگردانده است و از آن‌جایی که جزو سایت‌های تحریمی هم نیست، آدرس سرورهای `us1.shecan.ir` را به ما نداده است.

۴. خیر همان طور که در بالا توضیح داده شد، روش کار شکن بدین صورت است که لیستی از سایت‌های تحریم شده دارد و برای آن سایت‌ها، آی‌پی مربوط به سرورهای خود شکن را که در کشور دیگری مستقر هستند به ما بر می‌گرداند. بدین ترتیب، ریکوئست‌های ما به آن سایت از طریق سرورهای شکن که به نوعی نقش Man in the Middle را ایفا کرده است به آن سایت منتقل شده و جواب‌ها از طریق این سرور شکن به ما می‌رسد.

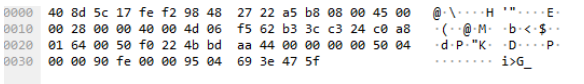
در مورد سایت‌های فیلتر شده، شکن یا عملکردی مانند DNS های ISP ها داشته و IP نامعتبری بر می‌گرداند و یا این که نهایتا IP واقعی آن سایت را به ما می‌دهد. حتی با وجود این IP واقعی هم امکان دسترسی به سایت ممکن نیست چون درخواست ما در راه به سرورهای ISP ها

می‌رسد و در آن جا با توجه به به این که مقصد آن جزو Blacklist سایت‌های فیلتر شده است، اجازه انتقال به آن داده نمی‌شود و Drop می‌شود. فیلترینگ سایتی نظیر فیسبوک صرفا در لایه DNS اعمال نشده، بلکه در لایه‌های دیگر هم اعمال شده است که اجازه انتقال بسته‌های درخواستی ما داده نشود تا حتی با داشتن آی‌پی سایت هم نتوان به آن دسترسی پیدا کرد.

۵. در قسمت قبلی هم یکی از IP های facebook نوشته شد. آی‌پی دیگری که با متصل بودن VPN فرانسه بدست آمد، 179.60.195.36 بود که واقعا IP ثبت شده شرکت Facebook بوده و موقعیت جغرافیایی آن هم در بلژیک است که همسایه فرانسه است. در صورت وصل بودن VPN، اطلاعات از طریق پروتکل ESP به سرورهای VPN ارسال شده و از طریق آن اطلاعات مربوط به فیسبوک دریافت می‌شود و سایت بدون مشکل باز می‌شود. با این حال در صورت قطع VPN و تلاش برای دسترسی به این آی‌پی وضعیت بسته‌ها مشابه زیر خواهد بود:

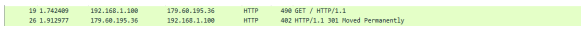


در ابتدا تعدادی بسته اولیه رد و بدل شده اما نتیجه نهایی به TCP RST ختم شده است و همچنین با بررسی محتویات پیام‌های TCP آمده متوجه می‌شویم که همگی آن‌ها بسیار کوتاه هستند و اطلاعات کافی سایت را در بر ندارند.



دلیل این موضوع هم این است که عملا فیلترینگ برای این سایت‌ها صرفا از لایه DNS نیست. بلکه به نوشته ویکی‌پدیا تکنولوژی Deep Packet Inspecting در بخش فیلترینگ به کار رفته که جزئیات بسته‌های رد و بدل شده را بررسی می‌کند. بدین ترتیب مواردی نظیر آدرس مبدا یا مقصد و همچنین محتویات و کلمات استفاده شده در متن پیام در صورت رمزنگاری نشدن آن می‌تواند باعث بشود که Packet مورد نظر به عنوان محتوای فیلتر شده شناسایی شده و بعد از رسیدن به ISP ها Drop شود و در مواردی نظیر بالا تنها شامل رسیدن بسته‌هایی با متحوای بسیار کم هستیم.

علاوه بر این **نکته مهم** دیگری هم وجود دارد و آن هم بررسی بسته http ارسال شده است. با بررسی این بسته‌ها به مورد زیر می‌رسیم:



پاسخ دریافت شده برای درخواست GET از این آدرس، کد 301 Moved Permanently است.

```
Hypertext Transfer Protocol
HTTP/1.1 301 Moved Permanently\r\n
Location: http://www.facebook.com/\r\n
```

```
Content-Type: text/html; charset="utf-8"\r\n
Date: Fri, 30 Apr 2021 15:11:44 GMT\r\n
Alt-Svc: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600\r\n
Connection: keep-alive\r\n
Content-Length: 0\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.170568000 seconds]
[Request in frame: 19]
[Request URI: http://179.60.195.36/]
```

آدرس جدید این سایت facebook.com اعلام شده است. در نتیجه دوباره سیستم سعی می‌کند از طریق DNS آدرس جدید را پیدا کند ولی در این زمینه هم با فیلترینگ مربوط به DNS رو به رو می‌شود و با آدرس 10.10.34.36 روبه‌رو می‌شود که آدرس معتبری نیست.