1. Introducción

El objetivo de este trabajo práctico es experimentar con el sistema de resolución de nombres DNS y el proceso de resolución de consultas.

Primero nos proponemos desarrollar una herramienta que nos permita consultar por los servidores de mail que atienden los correos electrónicos de algunas universidades en el mundo.

Luego, expondremos experimentos y sus resultados, donde veremos de manera empírica el funcionamiento de nuestra herramienta.

Por último, intentaremos experimentar con las zonas de autoridad de algunas universidades y analizar sus características.

2. Métodos y condiciones de los experimentos.

2.1. Código utilizado.

```python
from scapy.all import *

def makeRequestRecursive(domain, stop_at_first_answer = True):
    stack = [["198.41.0.4", 0],["198.41.0.4",0], ["199.9.14.201",0], ["192.33.4.12",0], ["199.7.91.13",0],
             ["192.203.230.10",0],["192.5.5.241",0], ["192.112.36.4",0], ["198.97.190.53",0],
             ["192.36.148.17",0], ["192.58.128.30",0] ,["193.0.14.129",0], ["199.7.83.42",0], ["202.12.27.33",0]]
    dns = DNS(rd=1,qd=DNSQR(qname= domain, qtype = "MX"))
    udp = UDP(sport=RandShort(), dport=53)
    amount_of_answers = 0
    set_authority_servers = set(())
    set_servers_non_responsive = set(())
    while(len(stack)>0):
        dst,height = stack.pop()
        ip = IP(dst= dst)

        answer = sr1( ip / udp / dns , verbose=0, timeout=10)

        if answer is not None and answer.haslayer(DNS):
            for i in range(answer[DNS].arcount):
                if answer[DNS].ar[i].type == 1:
                    set_authority_servers.add(dst)
                    if answer[DNS].ancount == 0:
                        stack.append([answer[DNS].ar[i].rdata, height +1])

            for i in range(answer[DNS].ancount):
                amount_of_answers += 1
                if stop_at_first_answer:
                    print ("La rta es: ",answer[DNS].an[i].rrname, answer[DNS].an[i].type,
                           [x.exchange for x in answer[DNS].an[i].iterpayloads()])
                    print("La altura es: ", height)
                    stack = []
        else:
            if dst not in set_servers_non_responsive:
                set_servers_non_responsive.add(dst)
                print("ip de servidor que no respondio: ", dst)
    if not stop_at_first_answer:
        print("Cantidad de Authority Servers: ",len(set_authority_servers))
        print("Cantidad de Authority Servers sin rta: ", len(set_servers_non_responsive))
        print("Cantidad de respuestas: ", amount_of_answers)
```

Para poder consultar por un mail server necesitamos poder realizar sucesivas consultas iterativas a distintos servidores.

La primera consulta siempre será hecha a un Root Name Server. En caso de que éste no pueda darnos una respuesta, obtendremos una lista de Authority Servers a los que podremos seguir consultando. Luego, la segunda consulta será hecha a alguna de estos. De aquí en más el proceso se repetirá hasta obtener una respuesta que nos indique que obtuvimos un registro MX o hasta que dejemos de obtener servidores autoritativos a los cuales preguntarles.

Para implementar esto utilizamos un stack. La idea es ir apilando las distintas IPs correspondientes a servidores a los cuales podemos consultar. Comienza con las IPs de los Root Name Servers que se encuentran en la consigna. Luego se desapila una de ellas y se le realiza la consulta iterativa. Si obtenemos a partir de ella una lista de servidores autoritativos, esta se añadirá al stack para poder continuar con las consultas. Nuevamente, se desapilará una IP del stack (que ahora corresponderá con la IP de un Authority Server) y se realizará la consulta, repitiéndose el procedimiento anterior.

El código nos permite terminar el método anterior cuando encontremos la primera respuesta de tipo 15 (es decir una vez que obtuvimos el registro MX del dominio de entrada), o continuarlo hasta que se hayamos agotado todos los servidores autoritativos a los que podíamos consultar.

A su vez contamos con dos Sets, uno se utiliza para almacenar los distintos servidores autoritativos a los que consultamos y el otro para los servidores que no responden. También mantenemos una variable para determinar

cuántas respuestas se obtuvieron al finalizar el proceso de consulta.

Por último, en el stack no solo guardamos las direcciones IP, si no que almacenamos un número, el cual representa la altura en el árbol de cada servidor, que luego nos servirá para poder determinar cuántos niveles de servidores DNS se recorrieron en las consultas antes de obtener la respuesta.

2.2. Descripción de las Universidades

Con el fin de probar cuáles son los servidores de mails que atienden los correros electrónicos de diversas entidades, seleccionamos las siguientes universidades para realizar el experimento:

1. Universidad de Murcia.
   - La universidad se encuentra en Murcia, España.
   - Dominio: um.es
   - Las corridas correspondientes a esta universidad se realizaron un Sábado a las 13hs.
2. Universidad de Yonsei.
   - La universidad se encuentra en Seúl, Corea del Sur.
   - Dominio: yonsei.ac.kr
   - Las corridas correspondientes a esta universidad se realizaron un Sábado a las 13hs.
3. Universidad de Trieste
   - La universidad se encuentra en Trieste, Italia.
   - Dominio: units.it
   - Las corridas correspondientes a esta universidad se realizaron un Sábado a las 13hs.

3. Resultados de los experimentos

En la siguiente tabla exponemos los resultados obtenidos:

Universidad	Niveles de Servidores	# Authority Servers	# Respuestas	# Servidores non responsive
España	3	572	416	1
Corea	3	19	1560	1
Italia	3	20	195	2

Figura 1: Resultados de los experimentos

En primer lugar, nos propusimos averiguar la cantidad de niveles de servidores DNS que se recorrieron hasta obtener la información solicitada. La tabla 1 muestra los resultados de los tres casos planteados anteriormente.

Como mencionamos en la sección 2, el código nos permitía obtener las respuestas junto con los niveles de servidores recorridos para las consultas hechas. Luego de correr la función con los dominios de las tres universidades, el número de niveles visitados fue 3 en todas ellas.

Por otro lado, nos planteamos indagar si todos los servidores DNS autoritativos que aparecen en las sucesivas respuestas responden a las consultas realizadas.

Observando nuevamente la tabla 1 podemos responder fácilmente que no. En las consultas de las tres universidades encontramos servidores autoritativos que no ofrecieron respuesta. En el caso de la universidad de Italia fueron dos servidores los que no respondieron (cuyas IPs son 194.146.106.30 y 192.36.148.17 respectivamente), mientras que en el caso de Corea del Sur y España hubo un único servidor no respondió (de IP 192.36.148.17). Notar que el servidor de IP 192.36.148.17 fue un servidor *non responsive* en todos los casos. Este además resulta ser el Root Server de nombre i.root-servers.net. Para este caso tenemos dos posibles hipótesis: una es que podría ser que el servidor esté caído, mientras que la otra es que nuestro provedor de Internet lo tenga bloqueado.

En cuanto a cantidad de nombres de servidores de mail de cada universidad, encontramos los siguientes:

Universidad de España

- mx01.puc.rediris.es
- mx02.puc.rediris.es

Universidad de Yonsei

- alt1.aspmx.l.google.com
- alt2.aspmx.l.google.com
- alt3.aspmx.l.google.com
- alt4.aspmx.l.google.com
- aspmx.l.google.com

Universidad de Italia

- mx.units.it

El dominio de la universidad de España es um.es. Dado que los nombres de los mails servers obtenidos no coinciden con el nombre del dominio, podemos afirmar que los mail servers de esta universidad no pertenecen al dominio de la misma.

Siendo que el dominio de la universidad de Corea del Sur es yonsei.ac.kr, podemos ver nuevamente que los nombres de los mails servers encontrados no se corresponden con este dominio. Nos parece interesante mencionar que cuando realizamos la corrida en la que consultábamos a todos los servidores autoritativos, algunos de ellos nos respondieron con los cinco mail servers mencionados, mientras que otros sólo con algunos de ellos.

El dominio de la universidad de Italia es units.it, por lo que podemos afirmar que el nombre del mail server pertence al dominio de la universidad.

Luego, para verificar si los servidores obtenidos estaban prendidos, efectuamos un *ping* a cada una de las IPs correspondientes a estos mail servers.

Los resultados de esta ejecución fueron los siguientes: para la universidad de España ninguna de las IPs nos respondió el *ping*, por lo que asumimos que están apagados. Por otro lado, las demás IPs sí nos respondieron, por lo que podemos afirmar que corresponden a dispositivos prendidos.

Por último, nos resultó interesante averiguar si las IPs de los servidores de correo coincidían con las IPs de los servidores web. Para esto, averiguamos cuáles eran las direcciones de los mail servers obtenidos anteriormente:

Universidad de España

- 130.206.19.130
- 130.206.19.162

Universidad de Corea

- 64.233.184.26
- 142.250.27.27
- 142.250.153.27
- 142.251.9.26

Universidad de Italia

- 140.105.48.195

Y averiguamos cuáles eran las direcciones IP de los web servers de las universidades:

- España: 155.54.212.103 - Corea del Sur: 165.132.13.38 - Italia: 140.105.48.2

Por un lado, notamos que para Corea del Sur y España las las IPs de los servidores web no coinciden con las IPs de los servidores de correo. Esto puede ser porque por ejemplo, en la universidad de Yonsei, el mail service es provisto por Google. Ademas, habíamos visto que los dominios de estas universidades no se correspondían con los nombres de sus mail servers.

Por otro lado, la universidad de Italia tiene una IP muy similar a la de su mail server. Probablemente la universidad de Italia tenga asignado un rango de IPs en el cual se encuentran estas dos direcciones. Mencionamos también que previamente habíamos observado que el dominio de la universidad contiene el nombre del mail server.

4. Consigna Opcional

Nuestro objetivo en este apartado es analizar la relación de cercanía entre los nameservers primarios y/o secundarios y las universidades a los que estos le prestan servicio. Para esto utilizamos la herramienta https://www.geodatatool.com de manera de efectuar la geolocalización de los nameservers en base a la dirección IP de los mismos.

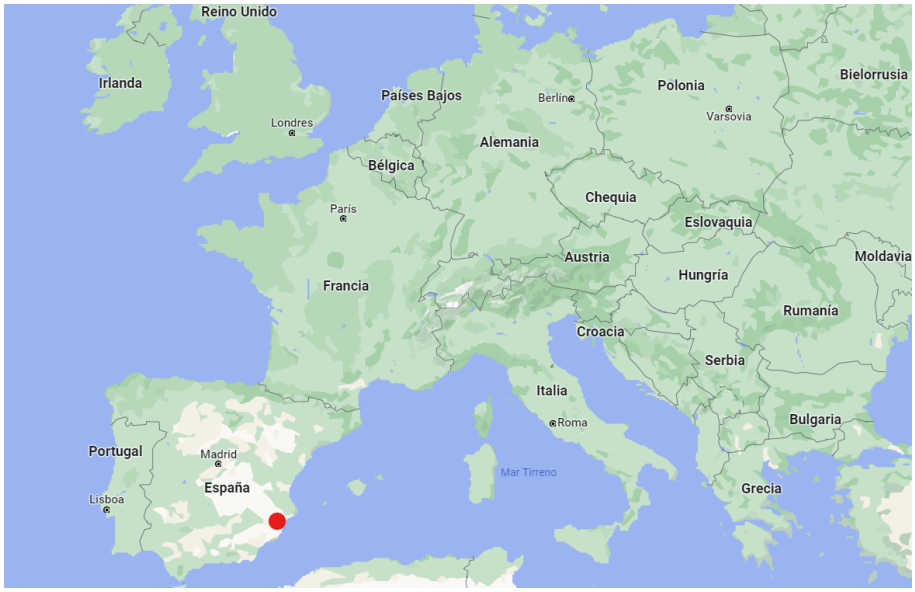
Para obtener los name servers de las universidades primero ejecutamos el comando dig *dominio.universidad* NS y luego el comando dig *nameserver* A con cada uno de los nameservers obtenidos con el comando anterior para obtener sus IPs.

Para mostrar los resultados utilizaremos mapas, los cuales tendrán marcados las ubicaciones de los nameservers y de las universidades con puntos rojos.

A continuación presentamos los resultados obtenidos:

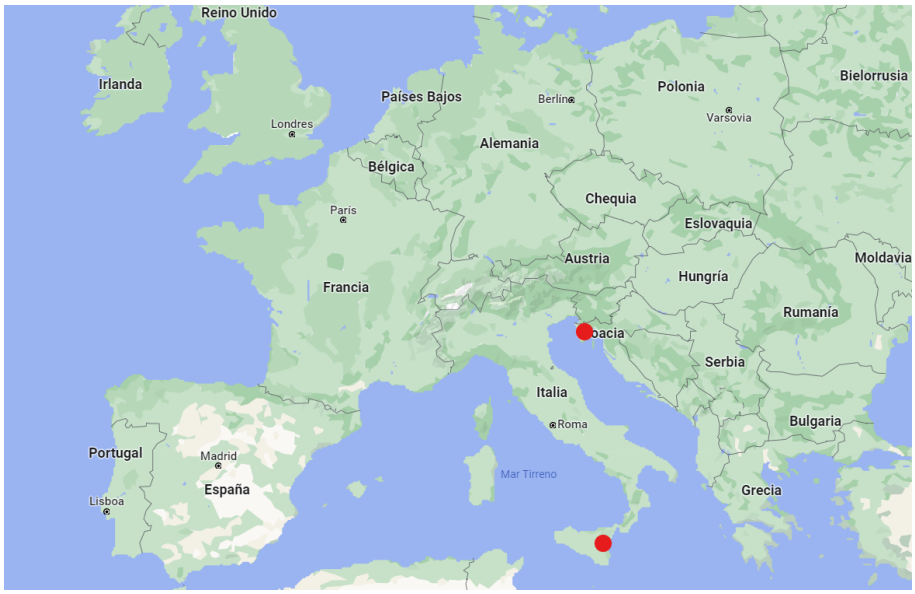
Universidad de Murcia (España)

Para esta universidad obtuvimos 2 nameservers: dns1.um.es (155.54.1.1) y dns2.um.es (155.54.1.2). La herramienta de geolocalización inidicó que ambos servidores se encuentran en Murcia, España, al igual que la universidad. Podemos ver esto en el siguiente mapa:



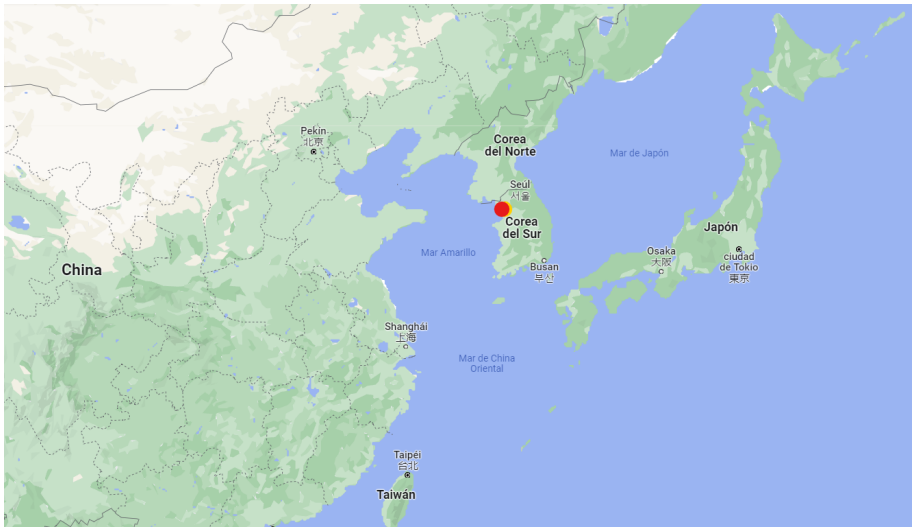
Universidad de Trieste (Italia)

Para esta universidad obtuvimos 3 nameservers autoritativos: ns1.units.it (140.105.114.22), ns2.units.it (140.105.114.33) y ns3.units.it (90.147.166.135). Estos servidores se encuentran en el país de Italia, dos de ellos se encuentran en la ciudad de Trieste, como la universidad, mientras que otro se ubica en Sicilia.



Universidad de Yonsei (Corea del Sur)

Para esta universidad obtuvimos 4 nameservers autoritativos: ns.yonsei.ac.kr (165.132.10.21), ns2.yonsei.ac.kr (165.132.5.21), ns3.yonsei.kr (165.132.237.21) y yumciris.yonsei.ac.kr (128.134.207.17) y, al igual que en el caso de España, obtuvimos que todos se ubican en la misma ciudad que la universidad: Seúl, Corea del Sur.



Luego de este análisis podemos afirmar que para todas las universidades la cercanía en general es muy estrecha, las ubicaciones de los nameservers se dan dentro de las mismas ciudades o ciudades muy cercanas a las universidades a las que estos atienden. El único servidor que notamos que no está tan próximo a su universidad asociada es el de Sicilia, sin embargo consideramos que su distancia sigue siendo pequeña dado que ambos encuentran en el mismo país.

Ahora intentaremos determinar si el subdominio de cada universidad define una zona de autoridad. Para poder hacer esto decidimos buscar los registros SOA de los subdominios de cada universidad, dados que estos son los que definen el comienzo de una zona de autoridad.

Utilizando el comando dig pudimos obtener los siguientes resutados para las universidades de Murcia, Trieste y Yonsei respectivamente:

```
mariana@mariana-Inspiron-5559:~$ dig um.es SOA +noall +ans
um.es.                  6816    IN      SOA     dns1.um.es. hostmaster.um.es. 2010124007 7200 720 2419200 7200
mariana@mariana-Inspiron-5559:~$ dig units.it SOA +noall +ans
units.it.               86400   IN      SOA     ns1.units.it. rete.units.it. 2022061100 86400 7200 604800 86400
mariana@mariana-Inspiron-5559:~$ dig yonsei.ac.kr SOA +noall +ans
yonsei.ac.kr.           3600    IN      SOA     ns.yonsei.ac.kr. network.yonsei.ac.kr. 2007120097 10800 900 604800 7200
```

De esta manera queda evidente que, al haber obtenido como respuesta al registro SOA en cada búsqueda efectuada, los tres subdominios de estas universidades definen zonas de autoridad. De lo contrario, el comando no nos hubiera devuelto un registro SOA.

Por último, nos proponemos investigar el subdominio de la carrera Computer Science dentro del dominio de la Universidad Princeton para ver si esta define una zona de autoridad y compararla con otras carreras de la misma, que en este caso serán Engineering Biology y Anthropology.

Los resultados de las queries para cada uno de los departamentos fueron los siguientes:

```
mariana@mariana-Inspiron-5559:~$ dig cs.princeton.edu SOA +noall +ans
cs.princeton.edu.       21600   IN      SOA     dns.cs.princeton.edu. hostmaster.cs.princeton.edu. 2022061000 1800 900 604800 21600
mariana@mariana-Inspiron-5559:~$ dig engbio.princeton.edu SOA +noall +ans
engbio.princeton.edu.   600     IN      CNAME   acquia-psb.princeton.edu.
mariana@mariana-Inspiron-5559:~$ dig anthropology.princeton.edu SOA +noall +ans
anthropology.princeton.edu. 577 IN      CNAME   acquia-psb.princeton.edu.
```

Podemos observar que para el subdominio del departamento de Computer Science, éste define una zona de autoridad ya que tiene un registro SOA. Por otro lado, notamos que los otros dos departamentos no tienen registros SOA, por lo que no definen zonas de autoridad.

5. Conclusiones

En este trabajo nos enfocamos en desarrollar una herramienta que nos permitiera realizar sucesivas consultas iterativas a los servidores DNS, particularmente para obtener los registros MX de dominios de distintas universidades en el mundo. Esta herramienta no solo nos permitió obtener los registros MX, sino que también nos resultó muy útil para poder analizar con mayor detenimiento las respuestas que obteníamos por cada consulta efectuada, de manera que conseguimos observar anomalías, saber el estado de los mail servers, determinar el comienzo de algunas zonas

de autoridad, y hasta realizar un análisis sobre la relación entre las ubicaciones de los servidores particulares que buscábamos y de las universidades a los que éstos atendían.

Dentro de las observaciones que nos parecieron interesantes, podemos destacar la manera en que los subdominios de cada universidad estaban determinados. Con esto nos referimos a que vimos casos con servidores de mail que se encontraban dentro del mismo dominio de la universidad, así como casos en que el servidor se correspondía a otro dominio, como la universidad de Yonsei con el servidor de mail de Google. Sin embargo, vimos que si bien estos dominios podían diferir, las distancias entre los servidores y las universidades eran bastante estrechas. Esto se podría explicar por lo específicos que resultaron ser los subdominios, ya que generalmente esto da una mayor posibilidad a que los nameservers se encuentren ubicados cerca de las mismas universidades. También podemos destacar cómo en nuestros resultados quedó en evidencia que cada servidor que representa a una universidad a su vez define una zona de autoridad. Más aun, en el estudio particular de Princeton, vimos como esta zona de autoridad pareciera englobar generalmente a los servidores de los departamentos de sus carreras, a excepción del departamento de Computer Science, el cual define su propia zona de autoridad.

A modo de cierre, creemos que gracias a la realización de este informe y las experimentaciones efectuadas, podemos reconocer que logramos profundizar sobre el sistema de resolución de nombres, de manera que obtuvimos un mayor entendimiento de cómo este funciona y cómo está conformado.