DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

# Taller III

## Taller 3: DNS

Teoría de las Comunicaciones
Segundo Cuatrimestre de 2022


| Integrante | LU | Correo electrónico |
|---|---|---|
| Francisco Jose Herrero | 136/19 | herrerofranciscojose@gmail.com |
| Nicolás Matías Sarfati | 690/13 | nicosarfa@hotmail.com |





**Facultad de Ciencias Exactas y Naturales**
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

# 1. Introducción

En este trabajo práctico nos proponemos a implementar y experimentar con el sistema de resolución de nombres: **DNS** y el proceso de resolución de consultas. Como primer paso, desarrollamos con la ayuda de Python3 y Scapy, una herramienta que nos permite consultar por los servidores de mail que atienden los correos electrónicos en algunas Universidades alrededor del mundo. Luego, procederemos a exponer experimentos con sus resultados, donde veremos de manera empírica el funcionamiento de nuestra herramienta. Por último, experimentaremos con las zonas de autoridad de dichas Universidades y analizaremos sus características.

# 2. Métodos y condiciones de los experimentos

## 2.1. Análisis del código utilizado

A continuación presentamos el código encargado de calcular el o los servidores de mail para las Universidades objetivo:

```python
def getMailExchange(domain, full_crawl=False):
    dns = DNS(rd=1,qd=DNSQR(qname=domain, qtype="MX"))
    udp = UDP(sport=RandShort(), dport=53)
    ips = [
        ("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)
    ]

    non_responsive_servers = set()
    authority_servers = set()
    amount_of_answers = 0

    while (len(ips) > 0):
        t = ips.pop()
        dst_ip, height = t[0], t[1]

        ip = IP(dst=dst_ip)
        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:
                    authority_servers.add(dst_ip)

                    if answer[DNS].ancount == 0:
                        ips.append([answer[DNS].ar[i].rdata, height + 1])

            for i in range(answer[DNS].ancount):
                amount_of_answers += 1

                if not full_crawl:
                    print("Los DNS para el servidor de mail del dominio: {} - Altura: {} - Tipo: {} son: {}".format(
                        answer[DNS].an[i].rrname,
                        height,
                        answer[DNS].an[i].type,
                        [p.exchange for p in answer[DNS].an[i].iterpayloads()]
                    ))
                    ips = []
        else:
            non_responsive_servers.add(dst_ip)

    if full_crawl:
        print("#Authority Servers: {} - {}".format(len(authority_servers), authority_servers))
        print("#Authority Servers NO RESPONSE: {} - {}".format(len(non_responsive_servers), non_responsive_servers))
        print("#Responses: {}".format(amount_of_answers))
```

Figura 1: Implementación propia del algoritmo de resolución de nombres

Para poder consultar por un servidor de mail, necesitamos realizar sucesivas consultas iterativas a todos los hops (Zonas / Authority Servers) que se encuentran en el camino. La primera consulta siempre será hecha a un Root Name Server. En caso de que este no posea la información necesaria para resolver la consulta (y en caso de ser posible), nos devolverá una lista de *Authority Servers* a los que deberemos seguir consultando. A partir de este punto, la segunda consulta será hecha a alguno de ellos. De ahora en más el proceso se repetirá hasta obtener una respuesta que nos indique que obtuvimos un registro MX o hasta que dejemos de obtener *Authority Servers* a los cuál consultarles.

Para lograr nuestro cometido, al momento de implementar el código, procedimos a utilizar un stack, el cuál nos permitió ir apilando las distintas IPs correspondientes a servidores a los cuales podemos consultar. El stack comienza con las IPs de los Root Name Servers[1], luego se desapila una de ellas y se le realiza la consulta iterativa. En caso de obtener a partir de dicho Root Name Server una lista de *Authority Servers*, estos se añadirán al stack que nos permitirá continuar con las consultas subsiguientes. Así, se desapilará una IP del stack, que ahora corresponderá con la IP de un *Authority Server* y se realizará el mismo procedimiento anterior.

El código expuesto en la figura 1, cuenta con la posibilidad de terminar ni bien se obtiene la primer respuesta de tipo MX (obtenida del dominio de entrada), o continuar hasta que se hayan agotado todos los *Authority Servers* intermedios.

A su vez, se mantiene una variable que nos permite cuantificar cuántas respuestas se obtuvieron al finalizar el proceso de consulta. Se almacenan dos sets, uno encargado de mantener registro de los distintos *Authority Servers* y otro que mantiene registro de aquellos servidores que no responden.

Por último, las direcciones IP son almacenadas junto con un número que representa la altura en el árbol de cada servidor, el cuál nos permitirá luego determinar cuántos niveles de servidores DNS se recorrieron en las consultas antes de obtener la respuesta buscada.

## 2.2. Descripción de las universidades

Con el fin de probar cuáles son los servidores de mail que atienden los correos electrónicos de diversas entidades, seleccionamos las siguientes Universidades para realizar la experimentación:

- Universidad de Uzbekistán
  - O'zbekiston Milliy Universiteti, se encuentra en Taskent - Uzbekistán [2]
  - Dominio: nuu.uz.
  - Las corridas correspondientes a esta Universidad se realizaron un día Jueves a las 11:45 ART.
- Universidad de Polonia
  - University of Silesia in Katowice, se encuentra en Katowice - Polonia [3]
  - Dominio: us.edu.pl.
  - Las corridas correspondientes a esta Universidad se realizaron un día Jueves a las 11:45 ART.
- Universidad de Rusia
  - National Research University, se encuentra en Moscú - Rusia [4]
  - Dominio: www.hse.ru.
  - Las corridas correspondientes a esta Universidad se realizaron un día Jueves a las 11:45 ART.

# 3. Resultados de los experimentos

En las siguientes tablas exponemos los resultados obtenidos del estudio de los dominios:

| Universidad | Niveles de Servidores | #Authority Servers | #Respuestas | #Non Responsive Servers |
|---|---|---|---|---|
| Uzbekistán | 3 | 21 | 182 | 0 |
| Polonia | 3 | 24 | 448 | 0 |
| Rusia | 3 | 21 | 582 | 1 |

Cuadro 1: Resultado de la experimentación

## 3.1. Análisis de resultados

A partir de los resultados obtenidos en la sección 3, podemos estudiar los distintos intermediarios que existen para obtener los servidores de mail a partir de un dominio.

Como primer medida, nos propusimos a averiguar la cantidad de niveles de servidores de DNS que se recorrieron hasta obtener la información requerida, observable en la tabla 1 para las tres Universidades estudiadas, en todos los casos, el número de niveles visitados fue **3**.

Luego, nos planteamos a indagar si todos los servidores DNS autoritativos que aparecen en las sucesivas respuestas responden a las consultas realizadas. Observando nuevamente la tabla 1, se puede observar que unicamente para el caso de la Universidad de Rusia no obtuvimos respuesta, siendo el mismo de IP: **92.242.58.5**. Para este caso, tuvimos dos tipos de sospechas, o bien que dicha IP se encontraba bloqueada por nuestro proveedor de Internet o que el servidor se encontraba caído o poseía el protocolo de ICMP deshabilitado. Buscando alternativas online [5] para responder a tal incertidumbre, se puede observar que el servidor en cuestión tampoco pareciera responder, por lo que se confirma la teoría de encontrarse caído o con el protocolo de ICMP deshabilitado.

Respecto a los distintos nombres de servidores de mail que encontramos para cada Universidad, fueron los siguientes:

- **Universidad de Uzbekistán**:
  - mx.yandex.net.
- **Universidad de Polonia**:
  - d69205b.ess.barracudanetworks.com.
  - d69205a.ess.barracudanetworks.com.
- **Universidad de Rusia**:
  - mg2.hse.ru.
  - mg1.hse.ru.

Se puede afirmar que tanto para el caso de la Universidad de Uzbekistán como la de Polonia, ninguna de ellas posee los servidores de mail como parte de su propio dominio y utilizan soluciones externas como Yandex[6] y Barracuda Networks[7], empresas externas que proveen soluciones informáticas.

Sólo para el caso de la Universidad de Rusia, podemos afirmar que es ella misma quien posee los Servidores de Mail dentro de su propio dominio, ya que coincide con la url de la Universidad.

Por otro lado, para verificar si los servidores de mail obtenidos estaban operativos, utilizamos el protocolo **ICMP** a través del comando **ping** contra cada uno de ellos, pero dado que el servidor podría estar operativo y sin embargo no responder a dichos tipos de mensajes (tal como vimos en el taller anterior), utilizamos también el comando **telnet** intentando conectarnos hacia alguno de los típicos puertos de los Servidores de Mail [8]:

| Puerto | Finalidad |
|---|---|
| 25 | Protocolo simple de transferencia de email |
| 465 | SMTP autenticado con SSL |
| 587/588 | Envío de mensajes de email |
| 2525 | El puerto alternativo |

Cuadro 2: Puertos típicos de Servidores de Mail

Los resultados obtenidos fueron los siguientes:

- **Universidad de Uzbekistán**:
  - PING hacia **mx.yandex.net.** satisfactorio, nos repondió la IP: **77.88.21.249**
  - Telnet no respondió hacia ninguno de los puertos típicos.
- **Universidad de Polonia**:
  - PING hacia **d69205b.ess.barracudanetworks.com. y d69205a.ess.barracudanetworks.com.** nos respondió en ambos casos la IP: **209.222.82.255** pero sin respuesta de ICMP
  - Telnet hacia **209.222.82.255** y puerto **587**, nos respondió correctamente esperando mensajes de email entrante.
- **Universidad de Rusia**:
  - Ping hacia **mg2.hse.ru.** nos respondió la IP: **92.242.58.14**, pero sin respuesta de ICMP.
  - Ping hacia **mg1.hse.ru.** nos respondió la IP: **92.242.58.12**, pero sin respuesta de ICMP.
  - Telnet no respondió hacia ninguno de los puertos típicos.

Por último, nos resultó interesante averiguar si las IPs de los servidores de correo coincidían con las IPs de los Servidores Web y como era de esperarse, en ninguno de los casos las mismas coincidió, ya que hoy es bastante común por temas de seguridad, separar la infraestructura lo máximo posible aunque se trate de servidores más chicos en términos de hardware.

# 4. Consigna Opcional

## 4.1. Análisis geográfico

En esta sección analizamos la relación de cercanía entre los Name Servers primarios y/o secundarios con las Universidades a las que le prestan servicio.

Utilizamos la herramienta brindada por la cátedra: **GeoTraceRoute** [9], de manera de efectuar la geolocalización de los Name Servers en base a su dirección IP.

Para obtener los Name Servers y las IPs de una Universidad, utilizamos el comando **dig** con una serie de parámetros. Comenzamos obteniendo los Name Servers de una Universidad ejecutando el comando **dig *DOMINIO_UNIVERSIDAD* NS** y luego obtenemos sus IPs ejecutando el comando **dig *NAME_SERVER* A** con cada uno de los Name Servers obtenidos.

Para una clara exposición de resultados, utilizaremos los siguientes mapas que tendrán marcados en ellos las ubicaciones de los Name Servers y las Universidades.

### 4.1.1. Universidad de Uzbekistán

Para esta Universidad obtuvimos **2** Name Servers Autoritativos:

- **ns1.nuu.uz** (62.209.143.181)
- **ns2.nuu.uz** (62.209.143.181)

La Universidad posee la misma dirección IP que sus Name Server y como es esperable, ambos servidores se encuentran en la misma ciudad que la Universidad (ya que poseen la misma dirección IP), observable en el siguiente gráfico:

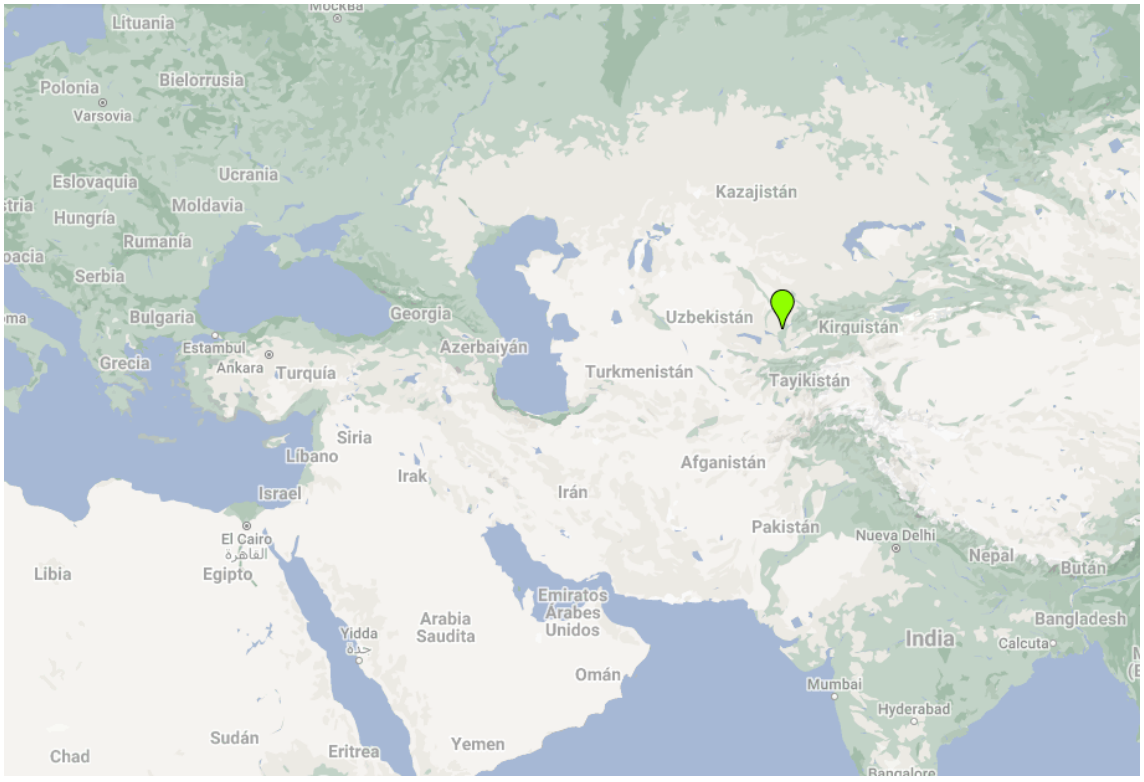


Figura 2: Cercania de los Name Servers que le prestan servicio a la Universidad de Uzbekistán

### 4.1.2. Universidad de Polonia

Para esta universidad obtuvimos **3** Name Servers Autoritativos:

- **dns1.us.edu.pl** (155.158.99.2): Ubicado en Katowice al igual que la Universidad
- **dns2.us.edu.pl** (155.158.102.7): Ubicado en Katowice al igual que la Universidad
- **cocos.fuw.edu.pl** (193.0.80.11): Ubicado en Warsaw

Resultados observables en el siguiente gráfico:

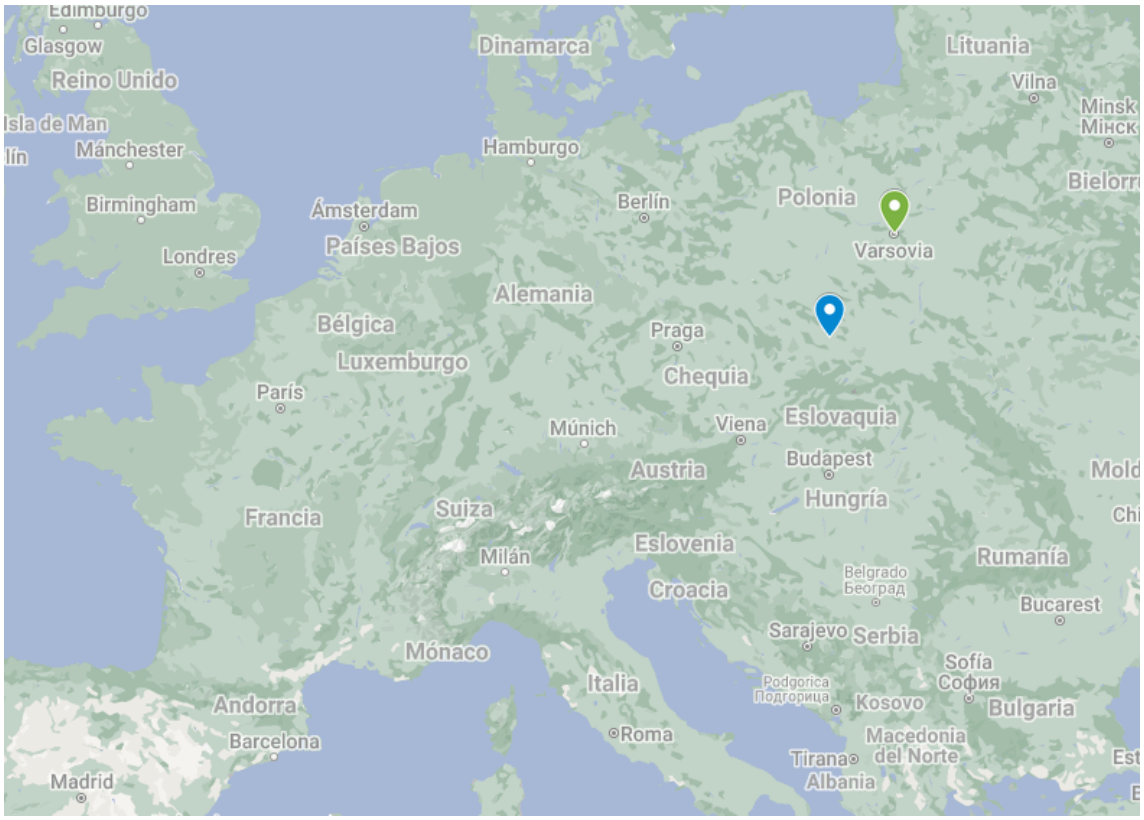


Figura 3: Cercania de los Name Servers que le prestan servicio a la Universidad de Polonia

### 4.1.3. Universidad de Rusia

Para esta universidad obtuvimos **5** Name Servers Autoritativos:

- **mx.hse.ru.** (92.242.58.5): Ubicado en Moscow al igual que la Universidad.
- **mx1.hse.ru.** (92.242.59.113): Ubicado en Moscow al igual que la Universidad.
- **mx2.hse.ru.** (45.89.226.137): Ubicado en Moscow al igual que la Universidad.
- **ns1.plusinfo.ru.** (No tiene dirección IP asignada): No puede ser rastreada por no contar con dirección IP.
- **ns2.plusinfo.ru.** (No tiene dirección IP asignada): No puede ser rastreada por no contar con dirección IP.

Resultados observables en el siguiente gráfico:

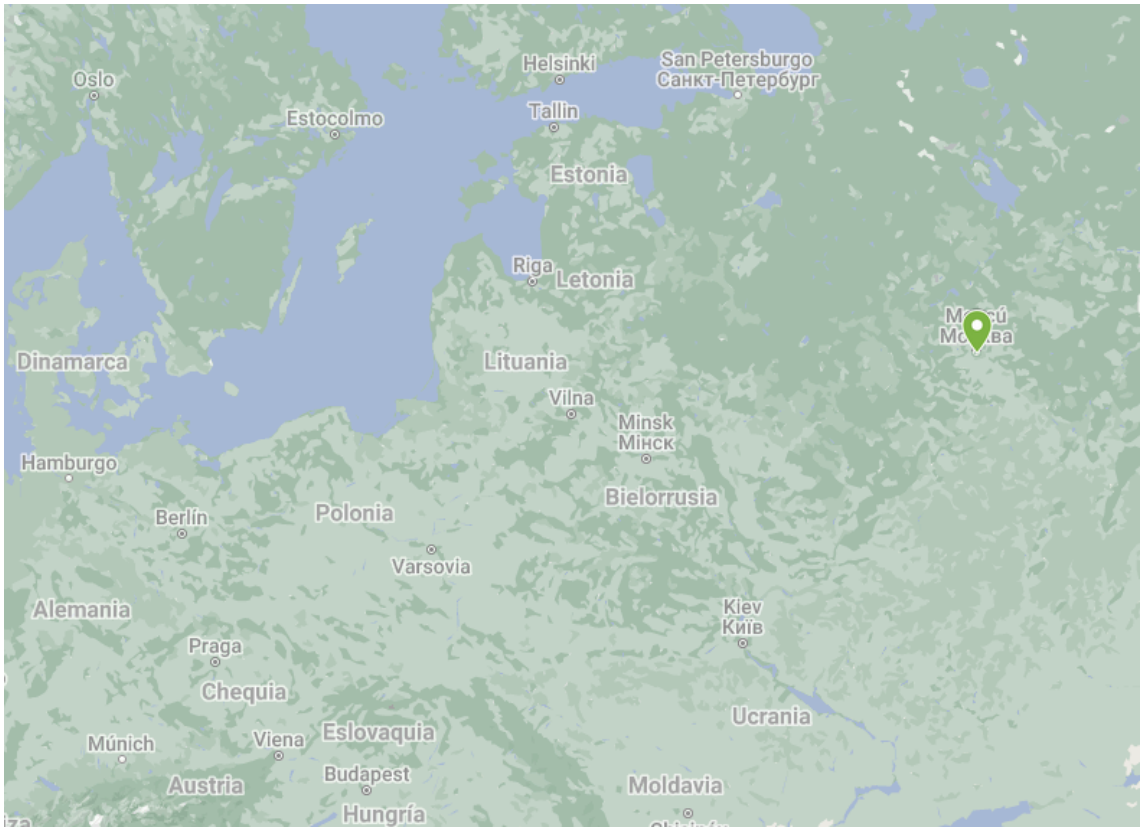


Figura 4: Cercania de los nameservers que le prestan servicio a la universidad de Rusia

## 4.2. Análisis de Zonas de Autoridad

Por otro lado, intentaremos determinar si el subdominio de cada Universidad examinada define una zona de autoridad, para ello, procederemos a analizar los registros **SOA** de los subdominios de cada Universidad ya que son ellos quienes definen el comienzo de una zona de autoridad.

Utilizando nuevamente el comando **dig**, logramos obtener los siguientes resultados para las Universidades de Uzbekistán, Polonia y Rusia:

```
 nicolas@desktop  ~  dig nuu.uz. SOA +noall +ans
nuu.uz.                 13383   IN      SOA     ns1.nuu.uz. root.nuu.uz. 2022031301 7200 3600 1209600 180
 nicolas@desktop  ~  dig us.edu.pl. SOA +noall +ans
us.edu.pl.              3600    IN      SOA     dns1.us.edu.pl. dns.us.edu.pl. 2022102707 3600 1800 1814400 86400
 nicolas@desktop  ~  dig www.hse.ru. SOA +noall +ans
www.hse.ru.             60      IN      CNAME   hse.ru.
hse.ru.                 60      IN      SOA     mx.hse.ru. net.hse.ru. 220064609 3600 3600 604800 86400
```

Figura 5: Resultado de Zonas de Autoridad para los subdominios de las Universidades destino.

Observando la figura 5, es evidente que al haber obtenido como respuesta el registro SOA en cada búsqueda realizada, los tres subdominios de estas Universidades definen Zonas de Autoridad. De lo contrario, el comando **dig** no nos hubiera devuelto un registro de dicho tipo.

Por último, nos propusimos a analizar el subdominio de la carrera de Ciencias de la Computación [10] dentro del dominio de la Universidad de Berkeley, para comprender si define una Zona de Autoridad y a su vez compararla con otras carreras dentro de la misma Universidad, que en este caso serán: Ingeniería Bio-Molecular [11] y Administración de Empresas [12].

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

```
 nicolas@desktop  ~  dig eecs.berkeley.edu. SOA +noall +ans
eecs.berkeley.edu.      86016   IN      SOA     ns.eecs.berkeley.edu. dns.eecs.berkeley.edu. 100011744 10800 3600 604800 86400
 nicolas@desktop  ~  dig chemistry.berkeley.edu. SOA +noall +ans
chemistry.berkeley.edu. 10800   IN      CNAME   live-chemistry-ob.pantheonsite.io.
live-chemistry-ob.pantheonsite.io. 600 IN CNAME fe2.edge.pantheon.io.
 nicolas@desktop  ~  dig haas.berkeley.edu. SOA +noall +ans
haas.berkeley.edu.      10800   IN      SOA     ewdc-vps-ib1.net.berkeley.edu. hostmaster.berkeley.edu. 2016442385 10800 1080 2419200 300
```

Figura 6: Resultado de Zonas de Autoridad para los subdominios de las Universidades de Berkeley.

Se puede observar en la figura 6, que para el subdominio del departamento de Computación y el de Administración de Empresas, estos definen una Zona de Autoridad, mientras que para el caso del departamento de Ingeniería Bio-Molecular no posee registrado el dominio SOA, por lo que no define una Zona de Autoridad.

# 5. Conclusiones

En este trabajo logramos implementar nuestra propia herramienta, que nos permitió realizar sucesivas consultas iterativas a los servidores DNS, para así obtener los registros MX de dominios de distintas Universidades del mundo.

Esta herramienta no solo fue de utilidad para obtener los registros MX, sino que tambien nos permitió analizar con mayor profundidad las respuestas que obtuvimos por cada consulta realizada, de manera tal que conseguimos observar anomalías, el estado de los servidores de mail, determinar el comienzo de algunas zonas de autoridad y hasta efectuar un análisis sobre la relación entre las ubicaciones de los Name Server y las Universidades en cuestión.

Dada la experiencia adquirida a lo largo de la investigación, nos encontramos capaces de responder las siguientes preguntas propuestas:

- **¿Cuántos niveles de servidores DNS se recorrieron en las sucesivas consultas hasta obtener la información solicitada?**

  Esta pregunta fue respondida a lo largo del análisis de los resultados en la sección 3.1, donde el número de niveles visitados fue en todos los casos **3**.

- **¿Todos los servidores DNS Autoritativos que aparecen en las sucesivas respuestas responden a las consultas realizadas?**

  Al igual que la pregunta anterior, fue respondida en la sección 3.1, fue Rusia el único que presentó un Servidor Autoritativo que no respondió.

- **¿Cuántos nombres de servidores de mail encontraron?, ¿Tienen nombres en el mismo dominio que la universidad?**

  Pregunta explicada con detalle en la sección 3.1, sólo en el caso de Rusia contaban con sus propios Servidores de email y poseen **dos**, mientras que para el caso de Uzbekistán (con un único Servidor de email) y Polonia (con dos Servidores), contaban con empresas externas que proveen soluciones informáticas.

- **¿Cuántas direcciones IP distintas hay? ¿Estas direcciones IP corresponden a dispositivos que están prendidos? (Hint: probar con ping si responden)**

  Analizado con las aplicaciones **PING** y **TELNET** en la sección 3.1.

- **¿Coinciden las IPs de los servidores de correo con las IPs de los servidores Web?**

  En ninguna de las Universidades, las IPs de los Servidores de email coincidió con las IPs de los Servidores Web.

- **¿Qué grado de cercanía tienen los nameservers a los servers de las universidades? Explique brevemente el resultado de los experimentos realizados.**

  Pregunta analizada con detalle en la sección 4.1, relación muy cercana entre la ubicación de la Universidad vs. la ubicación de los Name Servers.

- **Intente investigar el subdominio de la carrera Computer Science dentro del dominio de una universidad (Por ejemplo: csonline.eng.auburn.edu ) ¿Define una zona de autoridad? Compare con otras carreras de la misma universidad.**

  Punto también desarrollado en la sección 4.1, en donde se analizó la Universidad de Berkeley y tanto los dominios de la carrera de Ciencias de la Computación como la de Administración de Empresas presentaron ser Zonas de Autoridad, mientras que el caso de Ingeniería Bio-Molecular no lo era.

Por último y a modo de cierre, queremos destacar que en nuestros resultados quedó en evidencia que cada servidor que representa a una Universidad, a su vez define una Zona de Autoridad y que la herramienta estudiada para el análisis de resolución de nombres es imprescindible para lograr un mayor entendimiento empírico de una red global.

# Referencias


[1] URL: https://www.iana.org/domains/root/servers.

[2] URL: https://goo.gl/maps/jAgmbXqwrsQz2c9f8.

[3] URL: https://goo.gl/maps/tzBe5D6M2xzSNVf2A.

[4] URL: https://goo.gl/maps/Ao1ZZhrYC1S5NKTL9.

[5] URL: https://dnschecker.org/ping-ipv4.php.

[6] URL: https://es.wikipedia.org/wiki/Yandex.

[7] URL: https://en.wikipedia.org/wiki/Barracuda_Networks.

[8] URL: https://www.mailjet.com/es/blog/emailing/que-puerto-smtp-mailjet/#:~:text=Un%20puerto%20SMTP%20es%20un,%2C%20465%2C%20587%20y%202525..

[9] URL: https://geotraceroute.com/.

[10] URL: https://eecs.berkeley.edu/.

[11] URL: https://chemistry.berkeley.edu/cbe.

[12] URL: https://haas.berkeley.edu/.