

Redes: Capa de aplicación

Grupo: 96

Autores

Valentín Colato 15655/7

Nicolas Cesar Champane Peñalva 15974/9

Nahuel Bigurrarena 15782/3

Practica 2

HTTP

10. (Ejercicio de promoción) Resuelva los siguientes ejercicios justificando sus respuestas.

NOTA: *para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas. En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega.*

a. Investigue los distintos tipos de códigos de retorno de un servidor web y su significado. Considere que los mismos se clasifican en categorías (2XX, 3XX, 4XX, 5XX).

- **1XX son aquellos con fines informativos**
 - **100:** Este código indica que la petición que el navegador ha recibido está correcta.
 - **101:** Aquí el servidor ha aceptado los cambios de protocolo que se han propuesto por el navegador.
 - **102:** Este código significa que el servidor está procesando la petición del navegador pero todavía no ha terminado. Surge para evitar que el navegador piense que ha perdido la petición cuando no recibe ninguna respuesta.
- **2XX son códigos que indican éxito**
 - **200:** Este código indica que la página solicitada ha sido cargada de forma correcta.
 - **201:** La petición de carga ha sido completada y ha resultado en la creación de un nuevo recurso.
 - **202:** Aquí la petición elaborada ha sido aceptada para el procesamiento, pero este aún no ha sido completado por alguna prohibición.
 - **203:** Este código significa que la petición se ha completado con éxito, pero su contenido no se ha obtenido de la fuente originalmente solicitada sino de otro servidor.
- **3XX tratan sobre la redirección**
 - **301:** Este código indica una redirección permanente del dominio. Al ingresar a una página con el código 301 activo, inmediatamente el usuario será redireccionado a otro
 - **302:** Este es un código de redirección temporal, muy similar al anterior.
 - **303:** El servidor envía esta respuesta para dirigir al cliente a un nuevo recurso solicitado a otra dirección usando una petición GET.
 - **304:** (Not Modified) Esta es usada para propósitos de "caché". Le indica al cliente que la respuesta no ha sido modificada. Entonces, el cliente puede continuar usando la misma versión almacenada en su caché.
- **4XX son códigos de errores cometidos por parte del cliente**
 - **400:** El código 400 es un error que indica que la página a la que se desea ingresar no puede encontrarse debido a una falla en la digitación del usuario.

También se da cuando la página solicitada existió en algún momento pero ya no.

- **401:** Este código de error surge cuando la página está protegida con una contraseña y por tanto abre una nueva ventana para solicitar al usuario la información para iniciar sesión.
- **403:** Este código indica que la solicitud para entrar en un servidor no está permitida para el usuario. Se trata, generalmente, de páginas con contenidos exclusivo para usuarios registrados.
- **404:** Este error de "Not Found"/"No Encontrado" hace referencia, como el nombre lo indica, a las veces en que el navegador no encuentra la página que se está buscando porque no existe.
- **408:** En este código se indica que el tiempo de espera del servidor terminó para la conexión. Este error se genera cuando hay muchas personas solicitando el mismo sitio a la vez, lo que puede solucionarse refrescando la petición con F5, por ejemplo.
- **410:** El código 410 significa que el sitio solicitado ya no existe. Es un código de estado permanentemente activo por el administrador del sitio para que los buscadores lo eliminen de sus índices.
- **5XX son los problemas presentados por el servidor**
 - **500:** Este código alude a los errores internos, lo que significa que el servidor no puede generar el código HTML para devolver al usuario. Para arreglar este error, hay que revisar y localizar el archivo que lo está generando.
 - **503:** En este código de error se indica que el servidor no puede responder a la petición debido a que está congestionado o está en mantenimiento.
 - **504:** El error 504 significa que el tiempo de espera para devolver la página se ha agotado. Puede suceder porque la página tiene un código que no haya terminado de ejecutarse.
 - **509:** Este error indica que se ha superado el límite de ancho de banda disponible en el servidor para nuestra página web.

Estos son algunos de todos los códigos de retorno. Se pueden encontrar más en :

<https://developer.mozilla.org/es/docs/Web/HTTP/Status>

b. Utilizando curl, realice un requerimiento con el método HEAD al sitio www.redes.unlp.edu.ar e indique:

```
redes@redes:~$ curl www.redes.unlp.edu.ar -I
HTTP/1.1 200 OK
Date: Tue, 20 Oct 2020 22:42:00 GMT
Server: Apache/2.4.41 (Unix)
Last-Modified: Thu, 19 Mar 2020 14:39:34 GMT
ETag: "1322-5a136232cd580"
Accept-Ranges: bytes
Content-Length: 4898
Content-Type: text/html
```

i. ¿Qué información brinda la primer línea de la respuesta?

Devuelve la versión que se está utilizando (http 1.1 / 1.0 / 2.0), el código de retorno y un mensaje descriptivo del código de retorno.

ii. ¿Cuántos encabezados muestra la respuesta?

Se muestran 7 encabezados:

Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Content-Type

iii. ¿Qué servidor web está sirviendo la página?

Se aprecia en el encabezado de la respuesta "Server: Apache/2.4.41 (Unix)" que indica que el servidor que sirve la página es un Servidor Apache.

iv. ¿El acceso a la página solicitada fue exitoso o no?

Si fue exitoso ya que el código de retorno fue el 200 y este indica que la página solicitada ha sido cargada de forma correcta.

v. ¿Cuándo fue la última vez que se modificó la página?

El encabezado de Last-Modified indica la fecha de última modificación de la página la cual es : "Thu, 19 Mar 2020 14:39:34 GMT"

vi. Solicite la página nuevamente con curl usando GET, pero esta vez indique que quiere obtenerla sólo si la misma fue modificada en una fecha posterior a la que efectivamente fue modificada. ¿Cómo lo hace? ¿Qué resultado obtuvo? ¿Puede explicar para qué sirve?

Se hace agregando al encabezado el campo "If-Modified-Since: <day-name>, <day> <month> <year> <hour>:<minute>:<second> GMT"

El método para obtener la página si fue modificada en una fecha posterior a la que efectivamente fue modificada es :

```
curl -v www.redes.unlp.edu.ar -H 'If-Modified-Since: Thu, 19 Mar 2020 14:39:34 GMT'
```

El resultado que obtuve fue un código de retorno "304 Not Modified"

(304: (Not Modified) Esta es usada para propósitos de "caché". Le indica al cliente que la respuesta no ha sido modificada. Entonces, el cliente puede continuar usando la misma versión almacenada en su caché.)

Sirve para poder obtener páginas si la fecha Last-Modified del recurso remoto es más reciente que la dada en este encabezado.

c. Utilizando curl, acceda al sitio www.redes.unlp.edu.ar/restringido/index.php y siga las instrucciones y las pistas que vaya recibiendo hasta obtener la respuesta final. Será de utilidad para resolver este ejercicio poder analizar tanto el contenido de cada página como los encabezados. Para la entrega de promoción, adjunte todos los comandos que ejecutó junto con una explicación de cuáles fueron los diferentes indicios que lo llevaron a tomar cada decisión.

Aclaración: Las siguientes fotos fueron tomadas el día de la revisión por eso pueden no coincidir algunos valores.

1.

```
redes@redes:~$ curl -v www.redes.unlp.edu.ar/restringido/index.php
* Hostname was NOT found in DNS cache
*   Trying 172.28.0.50...
* Connected to www.redes.unlp.edu.ar (172.28.0.50) port 80 (#0)
> GET /restringido/index.php HTTP/1.1
> User-Agent: curl/7.38.0
> Host: www.redes.unlp.edu.ar
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Date: Tue, 20 Oct 2020 22:47:13 GMT
* Server Apache/2.4.41 (Unix) is not blacklisted
< Server: Apache/2.4.41 (Unix)
< WWW-Authenticate: Basic realm="Authentication Required"
< Last-Modified: Tue, 17 Mar 2020 15:16:01 GMT
< ETag: "cb-5a10e69d90e40"
< Accept-Ranges: bytes
< Content-Length: 203
< Content-Type: text/html
<
<h1>Acceso restringido</h1>

<p>Para acceder al contenido es necesario autenticarse. Para obtener los datos de acceso seguir las instrucciones detalladas en www.redes.unlp.edu.ar/obtener-usuario.php</p>
* Connection #0 to host www.redes.unlp.edu.ar left intact
```

curl -v www.redes.unlp.edu.ar/restringido/index.php

Utilizamos este comando y devolvió el código de error 401 Unauthorized.

Y obtuvimos este contenido :

<h1>Acceso restringido</h1>

<p>Para acceder al contenido es necesario autenticarse. Para obtener los datos de acceso seguir las instrucciones detalladas en www.redes.unlp.edu.ar/obtener-usuario.php</p>

2.

```
redes@redes:~$ curl -v www.redes.unlp.edu.ar/obtener-usuario.php
* Hostname was NOT found in DNS cache
*   Trying 172.28.0.50...
* Connected to www.redes.unlp.edu.ar (172.28.0.50) port 80 (#0)
> GET /obtener-usuario.php HTTP/1.1
> User-Agent: curl/7.38.0
> Host: www.redes.unlp.edu.ar
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 20 Oct 2020 22:53:05 GMT
* Server Apache/2.4.41 (Unix) is not blacklisted
< Server: Apache/2.4.41 (Unix)
< X-Powered-By: PHP/7.3.15
< Content-Length: 147
< Content-Type: text/html; charset=UTF-8
<
<p>Para obtener el usuario y la contraseña haga un requerimiento a esta página seteando el encabezado 'Usuario-Redes' con el valor 'obtener'</p>
* Connection #0 to host www.redes.unlp.edu.ar left intact
```

curl -v www.redes.unlp.edu.ar/obtener-usuario.php

Con este comando no obtuvimos error y devolvió:

<p>Para obtener el usuario y la contraseña haga un requerimiento a esta página seteando el encabezado 'Usuario-Redes' con el valor 'obtener'</p>

3.

```
redes@redes:~$ curl -v www.redes.unlp.edu.ar/obtener-usuario.php -H 'Usuario-Redes: obtener'
* Hostname was NOT found in DNS cache
*   Trying 172.28.0.50...
* Connected to www.redes.unlp.edu.ar (172.28.0.50) port 80 (#0)
> GET /obtener-usuario.php HTTP/1.1
> User-Agent: curl/7.38.0
> Host: www.redes.unlp.edu.ar
> Accept: */*
> Usuario-Redes: obtener
>
< HTTP/1.1 200 OK
< Date: Tue, 20 Oct 2020 23:00:28 GMT
* Server Apache/2.4.41 (Unix) is not blacklisted
< Server: Apache/2.4.41 (Unix)
< X-Powered-By: PHP/7.3.15
< Content-Length: 286
< Content-Type: text/html; charset=UTF-8
<
<p>Bien hecho! Los datos para ingresar son:
    Usuario: redes
    Contraseña: RYC
    Ahora vuelva a acceder a la página inicial con los datos anteriores.
    PISTA: Investigue el uso del encabezado Authorization para el método Basic. El comando base64 puede ser de ayuda!</p>
* Connection #0 to host www.redes.unlp.edu.ar left intact
```

Utilizamos el siguiente comando:

```
curl -v www.redes.unlp.edu.ar/obtener-usuario.php -H 'Usuario-Redes: obtener'
```

Obtuvimos:

<p>Bien hecho! Los datos para ingresar son:

Usuario: redes

Contraseña: RYC

Ahora vuelva a acceder a la página inicial con los datos anteriores.

PISTA: Investigue el uso del encabezado Authorization para el método Basic. El comando base64 puede ser de ayuda!</p>

La cabecera de petición **Authorization** contiene las credenciales para autenticar a un usuario en un servidor.

El encabezado es de la siguiente forma:

Authorization: <tipo> <credenciales>

<tipo>

Tipo de Autenticación. Un tipo común es "Basic". Otros tipos:

- IANA registry of Authentication schemes
- Authentication for AWS servers (AWS4-HMAC-SHA256)

<credenciales>

Si se utiliza el esquema de la autenticación "Basic", las credenciales son construidas de esta forma:

- El usuario y la contraseña se combinan con dos puntos (aladdin:opensesame).
- El string resultante está basado en la codificación base64 (YWxhZGRpbjpvGVuc2VzYW1l).

Para codificar en base64 el usuario y contraseña utilice el siguiente comando:

```
echo -n redes:RYC | base64
```

Devolvió:

```
cmVkZXM6UllD
```

(Utilizo -n para quitar el \n)

4.

```
redes@redes:~$ curl -v www.redes.unlp.edu.ar/restringido/index.php -H 'Authorization: Basic cmVkZXM6UllD'
* Hostname was NOT found in DNS cache
* Trying 172.28.0.50...
* Connected to www.redes.unlp.edu.ar (172.28.0.50) port 80 (#0)
> GET /restringido/index.php HTTP/1.1
> User-Agent: curl/7.38.0
> Host: www.redes.unlp.edu.ar
> Accept: */*
> Authorization: Basic cmVkZXM6UllD
>
< HTTP/1.1 302 Found
< Date: Tue, 20 Oct 2020 23:03:07 GMT
< Server: Apache/2.4.41 (Unix) is not blacklisted
< Server: Apache/2.4.41 (Unix)
< X-Powered-By: PHP/7.3.15
< Location: http://www.redes.unlp.edu.ar/restringido/the-end.php
< Content-Length: 230
< Content-Type: text/html; charset=UTF-8
<
<h1>Excelente!</h1>

<p>Para terminar el ejercicio deberás agregar en la entrega los datos que se muestran en la siguiente página.</p>
<p>ACLARACIÓN: la URL de la siguiente página está contenida en esta misma respuesta.</p>
* Connection #0 to host www.redes.unlp.edu.ar left intact
```

Usamos:

```
curl -v www.redes.unlp.edu.ar/restringido/index.php -H 'Authorization: Basic cmVkZXM6UllD'
```

Nos devolvió un 302 Found y el contenido:

```
<h1>Excelente!</h1>
```

```
<p>Para terminar el ejercicio deberás agregar en la entrega los datos que se muestran en la siguiente página.</p>
```

```
<p>ACLARACIÓN: la URL de la siguiente página está contenida en esta misma respuesta.</p>
```

La URL de la siguiente pagina es :

<http://www.redes.unlp.edu.ar/restringido/the-end.php>

Que se encuentra en el header "Location" de la respuesta

5.

```
redes@redes:~$ curl -v www.redes.unlp.edu.ar/restringido/the-end.php -H 'Authorization: Basic cmVkZXM6Ulld'
* Hostname was NOT found in DNS cache
* Trying 172.28.0.50...
* Connected to www.redes.unlp.edu.ar (172.28.0.50) port 80 (#0)
> GET /restringido/the-end.php HTTP/1.1
> User-Agent: curl/7.38.0
> Host: www.redes.unlp.edu.ar
> Accept: */*
> Authorization: Basic cmVkZXM6Ulld
<
HTTP/1.1 200 OK
< Date: Tue, 20 Oct 2020 23:05:11 GMT
* Server Apache/2.4.41 (Unix) is not blacklisted
< Server: Apache/2.4.41 (Unix)
< X-Powered-By: PHP/7.3.15
< Content-Length: 211
< Content-Type: text/html; charset=UTF-8
<
¡Felicitaciones, llegaste al final del ejercicio!
En la entrega adjuntá la siguiente información:
Fecha: 2020-10-20 23:05:11
* Connection #0 to host www.redes.unlp.edu.ar left intact
Verificación: b1bccb0dfa5ebc6bcf51d728aff2175431c46df00c02be1ae00047f972fb0971redes@redes:~$
```

Comando:

```
curl -v www.redes.unlp.edu.ar/restringido/the-end.php -H 'Authorization: Basic cmVkZXM6Ulld'
```

Adjunto la información obtenida en la página:

Fecha: 2020-09-19 22:21:54

Verificación:

4cbea7282dba0e92bebf5e2309f3d9f52d785179293ebe71da0c1c4d367afa71

Práctica 3

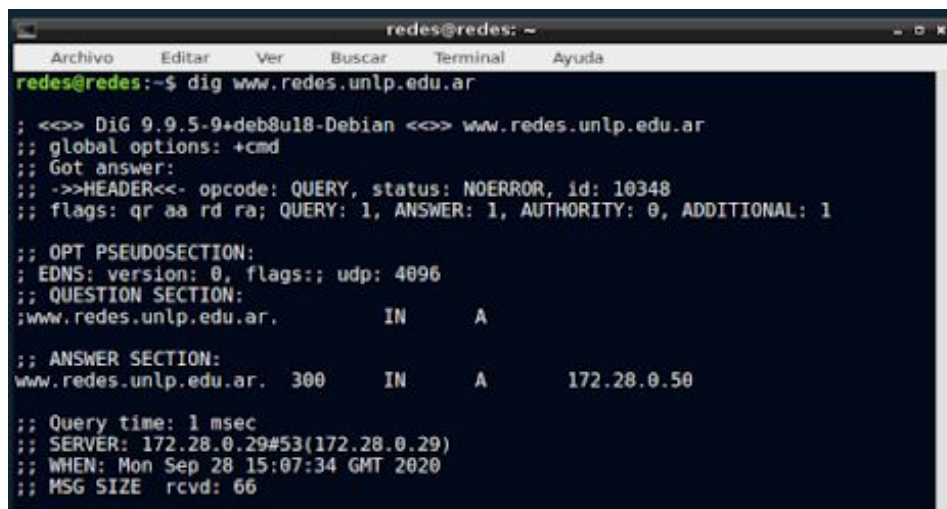
DNS

11. (Ejercicio de promoción) Responda y justifique los siguientes ejercicios.

NOTA: para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas.

En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega.

a. En la VM, utilice el comando dig para obtener la dirección IP del host `www.redes.unlp.edu.ar` y responda:



```
redes@redes: ~  
redes@redes:~$ dig www.redes.unlp.edu.ar  
  
; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.redes.unlp.edu.ar  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10348  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;www.redes.unlp.edu.ar.      IN      A  
  
;; ANSWER SECTION:  
www.redes.unlp.edu.ar. 300     IN      A      172.28.0.50  
  
;; Query time: 1 msec  
;; SERVER: 172.28.0.29#53(172.28.0.29)  
;; WHEN: Mon Sep 28 15:07:34 GMT 2020  
;; MSG SIZE rcvd: 66
```

i. ¿La solicitud fue recursiva? ¿Y la respuesta? ¿Cómo lo sabe?

Si la solicitud fue recursiva ya que tiene el flag **rd**.

rd: Recursion Desired, especifica que se solicita una consulta recursiva.

La respuesta fue recursiva ya que tiene el flag **ra**.

ra: Recursión Available. Denota en una respuesta que se ofrece la posibilidad de recursión.

ii. ¿Puede indicar si se trata de una respuesta autoritativa? ¿Qué significa que lo sea?

Si se puede indicar si se trata de una respuesta autoritativa. La respuesta fue autoritativa ya que contiene el flag **aa** :

AA:(Authoritative Answer) Informa de que es una respuesta autoritativa.

Esto significa que la respuesta DNS se ha producido desde el servidor DNS que tiene todo el archivo de información disponible para esa zona/dominio.

iii. ¿Cuál es la dirección IP del resolver utilizado? ¿Cómo lo sabe?

La dirección IP del resolver utilizado es : **172.28.0.29**.

Esto lo se ya que aparece como información al final de la respuesta que ofrece dig , en el apartado de SERVER: 172.28.0.26. Se realiza a esa dirección ip porque al no proporcionar ningún argumento de servidor al comando dig, esté consulta en el archivo **etc/resolv.conf** y utiliza los servidores DNS que figuran allí. En este archivo

cada línea llevará una única dirección IP correspondiente a un servidor DNS. Si queremos añadir más servidores DNS, podremos añadir hasta un máximo de 3 líneas. El orden es importante, ya que las consultas se enviarán al servidor de la primera línea, si este falla, se enviarán al servidor de la segunda línea y si este también falla, se enviarán al servidor de la tercera línea.

b. ¿Cuáles son los servidores de correo del dominio redes.unlp.edu.ar? ¿Por qué hay más de uno y qué significan los números que aparecen entre MX y el nombre? Si se quiere enviar un correo destinado a redes.unlp.edu.ar, ¿a qué servidor se le entregará? ¿En qué situación se le entregará al otro?

```
redes@redes:/etc$ dig redes.unlp.edu.ar -t mx

; <<> DiG 9.9.5-9+deb8u18-Debian <<> redes.unlp.edu.ar -t mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17287
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;redes.unlp.edu.ar.                IN      MX

;; ANSWER SECTION:
redes.unlp.edu.ar.                86400   IN      MX      5 mail.redes.unlp.edu.ar.
redes.unlp.edu.ar.                86400   IN      MX      10 mail2.redes.unlp.edu.ar.

;; ADDITIONAL SECTION:
mail.redes.unlp.edu.ar. 86400   IN      A       172.28.0.90
mail2.redes.unlp.edu.ar. 86400   IN      A       172.28.0.91

;; Query time: 0 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Mon Sep 28 17:20:08 GMT 2020
;; MSG SIZE rcvd: 121
```

Hay más de uno para mejorar la eficiencia ya que permite dividir las peticiones o envíos de email entre ambos dependiendo la cantidad de uso que tenga el servidor primario contra el secundario. Los servidores de correo del dominio redes.unlp.edu.ar son mail.redes.unlp.edu.ar (172.28.0.90) y mail2.redes.unlp.edu.ar (172.28.0.91). Los números que se encuentran entre MX y el nombre es un número positivo entre 0 y 65535, que determina la **preferencia**. El número de preferencia más pequeño tiene la mayor prioridad y será el primero en ser probado. Si se quiere enviar un correo destinado a redes.unlp.edu.ar se le entregará al servidor mail.redes.unlp.edu.ar(172.28.0.90) ya que tiene mayor prioridad por ser el que tiene menor número de preferencia. Para que se le entregará al otro servidor este tendría que tener mayor prioridad o sea menor número de preferencia.

c. ¿Cuáles son los servidores de DNS del dominio redes.unlp.edu.ar?

```
redes@redes:/etc$ dig redes.unlp.edu.ar NS

;<<> DiG 9.9.5-9+deb8u18-Debian <<> redes.unlp.edu.ar NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34132
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;redes.unlp.edu.ar.                IN      NS

;; ANSWER SECTION:
redes.unlp.edu.ar.                86400   IN      NS      ns-sv-b.redes.unlp.edu.ar.
redes.unlp.edu.ar.                86400   IN      NS      ns-sv-a.redes.unlp.edu.ar.

;; ADDITIONAL SECTION:
ns-sv-a.redes.unlp.edu.ar. 604800 IN      A       172.28.0.29
ns-sv-b.redes.unlp.edu.ar. 604800 IN      A       172.28.0.30

;; Query time: 1 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Sep 29 17:24:04 GMT 2020
;; MSG SIZE rcvd: 122
```

Los servidores de dns del dominio redes.unlp.edu.ar son:

ns-sv-b.redes.unlp.edu.ar.

ns-sv-a.redes.unlp.edu.ar.

Estos se obtienen con el comando: dig redes.unlp.edu.ar NS

d. Repita la consulta anterior cuatro veces más. ¿Qué observa? ¿Puede explicar a qué se debe?

Si se repite el comando anterior 4 veces más, podemos apreciar que el id de la consulta está variando y algunas veces se ve como cambian de orden los servidores en Answer section. Esto se debe a que va cambiando el orden de la respuesta para evitar que se acceda siempre al primer servidor de la lista.

e. Observe la información que obtuvo al consultar por los servidores de DNS del dominio. En base a la salida, ¿es posible indicar cuál de ellos es el primario?

No se puede indicar cual de ellos es el primario ya que no se tiene ninguna información especial que lo indique con el comando utilizado.

f. Consulte por el registro SOA del dominio y responda.

```
redes@redes:/etc$ dig redes.unlp.edu.ar SOA

;<<> DiG 9.9.5-9+deb8u18-Debian <<> redes.unlp.edu.ar SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32580
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;redes.unlp.edu.ar.                IN      SOA

;; ANSWER SECTION:
redes.unlp.edu.ar.                86400   IN      SOA      ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 86400

;; Query time: 1 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Sep 29 17:48:58 GMT 2020
;; MSG SIZE rcvd: 95
```

i. ¿Puede ahora determinar cuál es el servidor de DNS primario?

Si ahora se podría determinar el servidor primario, ya que la línea de Answer section, que indica el servidor DNS primario de la zona, responsable del mantenimiento de la información de la misma. Este es el ns-sv-b.redes.unlp.edu.ar

ii. ¿Cuál es el número de serie, qué convención sigue y en qué casos es importante actualizarlo?

El numero de serie del servidor **2020031700**.

Este valor en el campo RDATA del registro SOA se usa para indicar cambios de zona. Debe ser incrementado siempre que se realice cualquier modificación en los datos de zona.

iii. ¿Qué valor tiene el TTL de caché negativa y qué significa?

El valor que tiene el TTL de caché negativo es **86400**.

Este TTL negativo (Time To Live): Es el tiempo mínimo en el que se almacenan las respuestas negativas sobre una zona. Este tiempo es diferente al TTL de los RR.

Almacenamiento en caché negativo: TTL Las respuestas negativas (que suelen ocurrir cuando no existe un registro solicitado) también se pueden almacenar en caché en servidores no autorizados. Este campo se parece a un TTL básico, pero establece especialmente el valor de las respuestas TTL negativas. Se recomiendan pequeños periodos de tiempo (15min a 2h).

g. Indique qué valor tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar.

```
;; MSG SIZE rcvd: 105
redes@redes:/etc$ dig saludo.redes.unlp.edu.ar TXT
; <<> DiG 9.9.5-9+deb8u18-Debian <<> saludo.redes.unlp.edu.ar TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52991
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;saludo.redes.unlp.edu.ar.      IN      TXT
;; ANSWER SECTION:
saludo.redes.unlp.edu.ar. 86400 IN      TXT      "HOLA"
;; Query time: 1 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Sep 29 18:01:57 GMT 2020
;; MSG SIZE rcvd: 70
```

El valor que tiene el registro TXT de saludo.redes.unlp.edu.ar "HOLA"

h. Utilizando dig, solicite la transferencia de zona de redes.unlp.edu.ar, analice la salida y responda.

```
redes@redes:/etc$ dig axfr redes.unlp.edu.ar @ns-sv-a.redes.unlp.edu.ar
; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> axfr redes.unlp.edu.ar @ns-sv-a.redes.unlp.edu.ar
;; global options: +cmd
redes.unlp.edu.ar. 86400 IN SOA ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 86400
redes.unlp.edu.ar. 86400 IN NS ns-sv-a.redes.unlp.edu.ar.
redes.unlp.edu.ar. 86400 IN NS ns-sv-b.redes.unlp.edu.ar.
redes.unlp.edu.ar. 86400 IN MX 5 mail.redes.unlp.edu.ar.
redes.unlp.edu.ar. 86400 IN MX 10 mail2.redes.unlp.edu.ar.
ftp.redes.unlp.edu.ar. 86400 IN CNAME www.redes.unlp.edu.ar.
mail.redes.unlp.edu.ar. 86400 IN A 172.28.0.90
mail2.redes.unlp.edu.ar. 86400 IN A 172.28.0.91
ns-sv-a.redes.unlp.edu.ar. 604800 IN A 172.28.0.29
ns-sv-b.redes.unlp.edu.ar. 604800 IN A 172.28.0.30
practica.redes.unlp.edu.ar. 86400 IN NS ns1.practica.redes.unlp.edu.ar.
practica.redes.unlp.edu.ar. 86400 IN NS ns2.practica.redes.unlp.edu.ar.
ns1.practica.redes.unlp.edu.ar. 86400 IN A 172.28.0.120
ns2.practica.redes.unlp.edu.ar. 86400 IN A 172.28.0.121
saludo.redes.unlp.edu.ar. 86400 IN TXT "HOLA"
www.redes.unlp.edu.ar. 300 IN A 172.28.0.50
redes.unlp.edu.ar. 86400 IN SOA ns-sv-b.redes.unlp.edu.ar. root.redes.unlp.edu.ar. 2020031700 604800 86400 2419200 86400
;; Query time: 2 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Sep 29 18:14:41 GMT 2020
;; XFR size: 17 records (messages 1, bytes 413)
```

i. ¿Qué significan los números que aparecen antes de la palabra IN? ¿Cuál es su finalidad?

Es el campo TTL, un valor numérico que indica el tiempo en segundos que se cacheará el registro. Un valor 0 indica validez sólo para la transacción en curso y el registro asociado no será almacenado en caché. Indica por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen. Su finalidad es controlar el tiempo de vida en que estará almacenado en caché.

ii. ¿Cuántos registros NS observa? Compare la respuesta con los servidores de DNS del dominio redes.unlp.edu.ar que dio anteriormente. ¿Puede explicar a qué se debe la diferencia y qué significa?

Se puede observar 4 registros NS:

La diferencia entre la respuesta con los dominios de los servidores de DNS del dominio redes.unlp.edu.ar es que en la anterior respuesta devuelve solo los registros NS de redes.unlp.edu.ar y no de sus subdominios. En este último comando para solicitar la transferencia de zona de redes.unlp.edu.ar se observan todos los dominios y subdominios de este, por eso aparecen 2 NS más ya que hacen referencia a practica.redes.unlp.edu.ar.

i. Consulte por el registro A de www.redes.unlp.edu.ar y luego por el registro A de www.practica.redes.unlp.edu.ar. Observe los TTL de ambos. Repita la operación y compare el valor de los TTL de cada uno respecto de la respuesta anterior. ¿Puede explicar qué está ocurriendo? (Pista: observar los flags será de ayuda).

```
redes@redes:/etc$ dig www.practica.redes.unlp.edu.ar A
; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.practica.redes.unlp.edu.ar A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65007
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.practica.redes.unlp.edu.ar.      IN      A

;; ANSWER SECTION:
www.practica.redes.unlp.edu.ar. 35 IN    A      172.28.0.10

;; Query time: 2 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Sep 29 18:31:56 GMT 2020
;; MSG SIZE rcvd: 75

redes@redes:/etc$ dig www.redes.unlp.edu.ar A
; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.redes.unlp.edu.ar A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60941
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.redes.unlp.edu.ar.      IN      A

;; ANSWER SECTION:
www.redes.unlp.edu.ar. 300 IN    A      172.28.0.50

;; Query time: 1 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Tue Sep 29 18:32:02 GMT 2020
;; MSG SIZE rcvd: 66
```

Lo que está ocurriendo es que en el el servidor de www.practica.redes.unlp.edu.ar el TTL va decrementando desde 60 a 0 . Y en cambio en el servidor de www.redes.unlp.edu.ar el TTL es fijo de 300. La diferencia entre ambas operaciones es que la operación de www.redes.unlp.edu.ar es autoritativa y la otra no lo es.

Esto ocurre ya que los **servidores DNS** mantienen en **memoria caché**, si es que están configurados para ello, las respuestas a las preguntas que realizan a otros servidores, con un TTL (Time To Live) que indica el tiempo de vida que va a tener esa respuesta en el servidor.

Como la pregunta que se le realiza a 172.28.0.29 no es autoritativa sobre www.practica.redes.unlp.edu.ar entonces este realiza una consulta recursiva para obtener la ip, entonces almacena en memoria caché la respuesta obtenida del otro servidor por X tiempo definido por el TTL.

Práctica 4

Correo Electrónico

4. **(Ejercicio de promoción)** Utilizando la herramienta Swaks, envíe un correo electrónico con las siguientes características:

NOTA: para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas. En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega.

- Dirección destino: Dirección de correo de alumnoimap@redes.unlp.edu.ar
- Dirección origen: Dirección de correo de uno de los integrantes del grupo
- Asunto: SMTP-<Número de grupo>
- Archivo adjunto: PDF del enunciado de la práctica
- Cuerpo del mensaje: Nombres de los integrantes del grupo

a. Analice tanto la salida del comando swaks como los fuentes del mensaje recibido para responder las siguientes preguntas:

swaks --to alumnoimap@redes.unlp.edu.ar --from nahuel.bigu@gmail.com --header "Subject: SMTP-96" --body "Nahuel,Nicolas y Valentin" --attach p04.pdf

```
redes@redes:~/Descargas$ swaks --to alumnoimap@redes.unlp.edu.ar --from nahuel.bigu@gmail.com --header "Subject: SMTP-96" --body "Nahuel,Nicolas,Valentin" --attach p04.pdf
=== Trying mail.redes.unlp.edu.ar:25...
=== Connected to mail.redes.unlp.edu.ar.
<- 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
-> EHLO redes
<- 250-mail.redes.unlp.edu.ar
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-VRFY
<- 250-ETRN
<- 250-STARTTLS
<- 250-ENHANCEDSTATUSCODES
<- 250-8BITMIME
<- 250-DSN
<- 250 CHUNKING
-> MAIL FROM:<nahuel.bigu@gmail.com>
<- 250 2.1.0 Ok
-> RCPT TO:<alumnoimap@redes.unlp.edu.ar>
<- 250 2.1.5 Ok
-> DATA
<- 354 End data with <CR><LF>.<CR><LF>
-> Date: Thu, 08 Oct 2020 12:31:01 +0000
-> To: alumnoimap@redes.unlp.edu.ar
-> From: nahuel.bigu@gmail.com
-> Subject: SMTP-96
-> Message-Id: <20201008123101.002441@redes>
-> X-Mailer: swaks v20190914.0 jetmore.org/john/code/swaks/
-> MIME-Version: 1.0
-> Content-Type: multipart/mixed; boundary="-----=_MIME_BOUNDARY_000_2441"
->
-> -----=_MIME_BOUNDARY_000_2441
-> Content-Type: text/plain
->
-> Nahuel,Nicolas,Valentin
-> -----=_MIME_BOUNDARY_000_2441
-> Content-Type: application/octet-stream; name="p04.pdf"
-> Content-Description: p04.pdf
-> Content-Disposition: attachment; filename="p04.pdf"
-> Content-Transfer-Encoding: BASE64
->
-> JVBERi0xLjUKJdDUxdGKNiAwIG9iag08PC9MZW5ndGggMTYyOCAgICAgIC9GaWx0ZXIvRmxhdGVE
-> ZWNvZGU+PgpzdHJlYW0KeNqtWntu3DYQfd+v0KMwiBleRSkvqZsmbYI63dSbAkWcB1qSX0Faaa0L
-> U/fr07zJ0t6NLBZYSeRw0HNMznAKHNwH0Ph19vNy9vIdY0GMkihcbC8CwhMYPiXGMVRFEiRoJgl
-> wXIVfAnfqlWax1AZh1lur5frskhVWtywiFV6SIYXduZN3TR5be/zMk+7xsgUKYyRSLAo/DPP8tYK
-> PNPwLq/mJAn7yuisKzs9qKSY4vnX5YfZ2+Xs22zL0AhFggTpavbLk4ymPsQYMSS0PhuJfCBFwwJ
-> zuC+DK5nn2bYobDv6tEhELE10B/DQ2G7JJJBFEtEIoFpANzkJ03AfGs4N+a+fEejgBCUCEHkWA1J
-> YDABJRFdNcZgmw31tZjLD4jTd0BJKSBSKJEeHC7Tvokrt0eVCMmvvYhWCKI8CISns530SNFk7
-> yBKGJN6QvYGNP/U3TJD5BZM8XDd1V6d1Wbf2uc3tte+KsvhPVU5KNfMkVPqBgdl2MK90Gj2ALlHb
-> mcwsFuFKFWXrhbrGqTTr0rKAUTf46Lbt/fYN30DwocjqxirLnGRqkHtH7Qbf4930ABs007ZiZix
-> jhvnNLGaPSN87L3unTB6yBLFFEurjR6BfCw7gZxuQe4d5FSMIadjyCkLS2VFmjzN100KajGDDlwN
```

i. ¿A qué corresponde la información enviada por el servidor destino como respuesta al comando EHLO? Elija dos de las opciones del listado e investigue la funcionalidad de la misma.

EHLO (Extended HELLO) en lugar de HELO (el Hello original del estándar). Un servidor puede por tanto responder con éxito (código 250), falla (código 550) o error (códigos 500, 501, 502, 504 o 421), dependiendo de su configuración. Un servidor ESMTP respondería el código 250 OK en una respuesta de varias líneas con su dominio y una lista de palabras clave para indicar las extensiones soportadas.

250-VRFY

Devuelve si la dirección de correo electrónico especificada es un destinatario válido. Una solicitud VRFY pide al servidor que verifique una dirección. Su parámetro puede ser una dirección codificada o un nombre de usuario en un formato definido por el servidor.

Si el servidor acepta la solicitud (código requerido 250, 251 o 252), puede proporcionar información sobre la dirección en un formato definido por el servidor. 250 normalmente significa que la dirección es válida, 251 normalmente significa que el correo a la dirección se reenvía y 252 significa que el servidor no sabe si la dirección es válida.

A menudo deshabilitado para evitar que los spammers prueben una lista de nombres de diccionario para crear una lista de destinatarios válidos.

250-PIPELINING

Indica compatibilidad con una secuencia de comandos sin esperar una respuesta a cada comando. Se supone que el servidor receptor procesa por lotes las respuestas. Se supone que el streaming se detiene con un comando que puede cambiar el estado del servidor SMTP receptor (como el comando DATA)

250-8BITMIME

Indica compatibilidad con el contenido del mensaje de correo codificado de 8 bits (en lugar de 7 bits), a través de la adición opcional de un parámetro al comando MAIL

ii. Indicar cuáles cabeceras fueron agregadas por la herramienta swaks.

La siguiente cabecera fue agregada por swaks:

X-Mailer: swaks v20190914.0 jetmore.org/john/code/swaks/

Esta línea X-Mailer en el encabezado del correo electrónico indica qué programa se utilizó para redactar y enviar el correo electrónico original.

Agregadas por swaks por el uso del comando --attach :

Content-Type: multipart/mixed; boundary="-----_MIME_BOUNDARY_000_2441"

Content-Type: application/octet-stream; name="p04.pdf"

Content-Description: p04.pdf

Content-Disposition: attachment; filename="p04.pdf"

Content-Transfer-Encoding: BASE64

iii. ¿Cuál es el message-id del correo enviado? ¿Quién asigna dicho valor?

Se aprecia en el encabezado message-id: <20201008123101.00241@redes>. Lo asigna normalmente el servidor de correo que envía el mensaje en nombre de su cliente de correo.

La técnica utilizada consiste en una marca de hora y fecha junto con el nombre de dominio del cliente.

iv. ¿Cuál es el software utilizado como servidor de correo electrónico?

El software utilizado es: "ESMTP Postfix (Lihuen-4.01/GNU)" una distribución desarrollada en Argentina por la Facultad de Informática de la Plata.

v. Adjunte la salida del comando swaks y los fuentes del correo electrónico.

```
=== Trying mail.redes.unlp.edu.ar:25...
=== Connected to mail.redes.unlp.edu.ar.
<- 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
-> EHLO redes
<- 250-mail.redes.unlp.edu.ar
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-VERFY
<- 250-ETRN
<- 250-STARTTLS
<- 250-ENHANCEDSTATUSCODES
<- 250-8BITMIME
<- 250-DSN
<- 250 CHUNKING
-> MAIL FROM:<nahuel.bigu@gmail.com>
<- 250 2.1.0 Ok
-> RCPT TO:<alumnoimap@redes.unlp.edu.ar>
<- 250 2.1.5 Ok
-> DATA
<- 354 End data with <CR><LF>.<CR><LF>
-> Date: Thu, 08 Oct 2020 23:05:46 +0000
-> To: alumnoimap@redes.unlp.edu.ar
-> From: nahuel.bigu@gmail.com
-> Subject: SMTP-96
-> Message-Id: <20201008230546.001659@redes>
-> X-Mailer: swaks v20190914.0 jetmore.org/john/code/swaks/
-> MIME-Version: 1.0
-> Content-Type: multipart/mixed; boundary="-----=_MIME_BOUNDARY_000_1659"
->
```

```

-> -----=_MIME_BOUNDARY_000_1659
-> Content-Type: text/plain
->
-> Nahuel,Nicolas y Valentin
-> -----=_MIME_BOUNDARY_000_1659
-> Content-Type: application/octet-stream; name="p04.pdf"
-> Content-Description: p04.pdf
-> Content-Disposition: attachment; filename="p04.pdf"
-> Content-Transfer-Encoding: BASE64
->
-> BASE64 ENCODED PDF....
->
-> -----=_MIME_BOUNDARY_000_1659--
->
->
-> .
<- 250 2.0.0 Ok: queued as D78D4189
-> QUIT
<- 221 2.0.0 Bye
=== Connection closed with remote host.

```

5. (Ejercicio de promoción) Descargue de la plataforma la captura de tráfico smtp.pcang y la salida del comando swaks smtp.swaks para responder y justificar los siguientes ejercicios.

NOTA: para quienes hagan la promoción, este será un ejercicio entregable. En la entrega deberán estar todas las preguntas respondidas y debidamente justificadas. En los puntos donde es necesario ejecutar comandos, los mismos deberán adjuntarse a la entrega.

a. ¿Por qué el contenido del mail no puede ser leído en la captura de tráfico?

No se puede leer ya que se utiliza STARTTLS . El hace que se utilice TLS para enviar los mensajes SMTP de forma segura (cifrado) .

b. Recupere el archivo adjunto a partir de la salida del comando de swaks para indicar de qué personaje se trata.

1. Copiamos del archivo smtp.swaks la imagen cifrada que estaba adjunta en un nuevo archivo "imagen"
2. Utilizamos el comando base64 para decodificarla utilizandolo con el parámetro -d
base64 -d imagen > imagen.png

