Redes de Computadoras II
DNS

NOMBRE: Daniel Alberto Vinzia

Usando dig para hacer consultas DNS

1. ¿Cuál es el nombre canónico del servidor web de GNU? ¿Cuál es su dirección IP?

El nombre canónico del servidor es *gnu.org* y su direccion ip es *209.51.188.116*

2. ¿Que puedes hacer con el resto de la respuesta?

Me da características de que fue enviado correctamente, el peso del mismo, me dice la versión del Dig, me muestra que fue enviado por UDP

3. ¿Cuál es la dirección IP del servidor DNS que respondió la consulta realizada en el paso 2? (Ayuda: la respuesta está disponible al final de la respuesta) ¿Quién es este servidor?

En el mensaje, en la parte final, se lee lo siguiente:

Server: 192.168.100.1·53(192.168.100.1) (UDP)

4. Sugiera una posible razón para tener un alias para este servidor. ¿Es posible verificar sus conclusiones? Si la respuesta es positiva, explique cómo.

Un servidor puede tener un alias para facilitar su identificación y acceso, especialmente cuando hay múltiples servidores en una red. Los alias permiten que los clientes se conecten a servidores con diferentes protocolos sin tener que especificar todos los detalles de la conexión, simplificando la administración.

5. ¿Cuales son los servidores de nombre DNS para el dominio "gnu.org"? ¿Cuáles son sus direcciones IP? ¿Cómo se puede constatar adicionalmente esta información? ¿Qué utilidad tiene hacerlo? (Ayuda: utilize el sitio www.whois.net o dnsquery.org y averigue para que se usan)

En **whois** nos marca los siguientes:

ns1.gnu.org

ns2.gnu.org

ns3.gnu.org

ns4.gnu.org

En **dnsquery** nos marca que ns4 es de ip 188.165.235.157

Podemos buscar un servidor más cercano para comunicarnos ya que cuando hacemos la consulta por **dnsquery**, las respuestas varían de los 1.87ms a 157.03ms

6. ¿Qué información adicional obtuvo del paso 4?

Al estar la información en varios servidores no dependemos de un solo lugar más vulnerable sino que la información se siente que está en toda la red y a el alcance de uno, haciendo que podamos comunicarnos con el servidor que mas nos convenga

```
dig www.gnu.org

; <<>> DiG 9.20.7 <<>> www.gnu.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31441
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.gnu.org.                   IN      A

;; ANSWER SECTION:
www.gnu.org.            1385    IN      A       209.51.188.116

;; Query time: 3 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Tue Apr 29 14:54:00 -03 2025
;; MSG SIZE  rcvd: 56
```

```
dig gnu.org NS

; <<>> DiG 9.20.7 <<>> gnu.org NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46127
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; COOKIE: 8694d2cac059d4e431b3525a681112753eb7de9ce35508f7 (good)
;; QUESTION SECTION:
;gnu.org.                       IN      NS

;; ANSWER SECTION:
gnu.org.                1800    IN      NS      ns1.gnu.org.
gnu.org.                1800    IN      NS      ns2.gnu.org.
gnu.org.                1800    IN      NS      ns4.gnu.org.

;; Query time: 279 msec
;; SERVER: 192.168.100.1#53(192.168.100.1) (UDP)
;; WHEN: Tue Apr 29 14:55:01 -03 2025
;; MSG SIZE  rcvd: 118
```

```
dig +trace www.gnu.org

; <<>> DiG 9.20.7 <<>> +trace www.gnu.org
;; global options: +cmd
.                       183080  IN      NS      e.root-servers.net.
.                       183080  IN      NS      g.root-servers.net.
.                       183080  IN      NS      m.root-servers.net.
.                       183080  IN      NS      h.root-servers.net.
.                       183080  IN      NS      a.root-servers.net.
.                       183080  IN      NS      f.root-servers.net.
.                       183080  IN      NS      d.root-servers.net.
.                       183080  IN      NS      k.root-servers.net.
.                       183080  IN      NS      c.root-servers.net.
.                       183080  IN      NS      l.root-servers.net.
.                       183080  IN      NS      b.root-servers.net.
.                       183080  IN      NS      j.root-servers.net.
.                       183080  IN      NS      i.root-servers.net.
.                       453926  IN      RRSIG   NS 8 0 518400 20250511210000 20250428200000 53148 . hbk40JRMgm291rKBkP/RDIcW3uRxdK9cpYeLaBQg8JgrYPG+gZRjoMP/ oH7/PI/ARu
eQdLkOlMF1mXfekhgHFoPr/8yfqjjk84PBadydthUxFQjd 1KIpssWod4tz14VPP5n4Jqn+Ny9iYgWWKVP5TQwAGdfmSMxWbGCfe+tg v7n+0WnHK25oLTmH/Wymy4VfhOvx2O/ZxvCD7A+wcB9BdB8EuOF8uO46 g7Fkir
m6m2enp10af7BZPTur39g1HcNbx5qpLZfn47GxgwZMO8xETRcp kw1H7BY88cd1fF7jarSGsaJniP8sdyHR+5uC2HmVwwtwTtjSoFamKm4/ 8nW1jA==
;; Received 1125 bytes from 192.168.100.1#53(192.168.100.1) in 16 ms

org.                    172800  IN      NS      a2.org.afilias-nst.info.
org.                    172800  IN      NS      b2.org.afilias-nst.org.
org.                    172800  IN      NS      d0.org.afilias-nst.org.
org.                    172800  IN      NS      a0.org.afilias-nst.info.
org.                    172800  IN      NS      b0.org.afilias-nst.org.
org.                    172800  IN      NS      c0.org.afilias-nst.info.
org.                    86400   IN      DS      26974 8 2 4FEDE294C53F438A158C41D39489CD78A86BEB0D8A0AEAFF14745C0D 16E1DE32
org.                    86400   IN      RRSIG   DS 8 1 86400 20250512050000 20250429040000 53148 . lPV0ZS+Y+Vc9fuCN6UaO5cSBrDLKkj3lrgFn6PTJ+mrWvyjeFG5VCH46 oiKYlTuuoVJ
zddka0bQA/oX65hV+GuulwSlnGhUd7M9XHwfcZz4PY3qQ TyylLX/Cgz/oHIwd6MiLknJZk/Cwwho3s1hLzhPKMRpFeeRvIpuk5Y4L Q1aZoQDbnzy2cM2VQDl9t3wdqmhvwplcFShhWhEaG++YdK89g5xe6EaK AEQa9He
MkAWSDE9BKOWy4R/eJ9J8tvR1Qt25E7eISWeXZWnK1kE0bPmi JhdhBxoJUDxjNbWSEvcfH6s04vJUD2ed2F1ePw0CAA6FqoN2lABWrbTH rR62Og==
;; Received 777 bytes from 2001:503:ba3e::2:30#53(a.root-servers.net) in 206 ms
```

```
gnu.org.                3600    IN      NS      ns1.gnu.org.
gnu.org.                3600    IN      NS      ns2.gnu.org.
gnu.org.                3600    IN      NS      ns4.gnu.org.
gdtpongmpok61u9lvnipqor8lra9l4t0.org. 3600 IN NSEC3 1 1 0 332539EE7F95C32A GDTREA8KMJ2RNEQEN4M2OGJ26KFSUKJ7 NS SOA RRSIG DNSKEY NSEC3PARAM
gdtpongmpok61u9lvnipqor8lra9l4t0.org. 3600 IN RRSIG NSEC3 8 2 3600 20250520175404 20250429165404 48111 org. TrLO1xDoxmX/POy2ckdrbY6HjYiZA886s5yP4txoSk4PrTzmBo4PgKR9 Yf
IS+tkhH842T+xfRawFKS/oAztLjSbqtmfDYXpnJu220yVpedFb7uqA tuO4APmrkw1sVxrpl2d741L5XE9HUSMh8m7P6mJ/yq3Q7WQNY8G9ik2J 7rs=
75u43m27modtpregu0d0merldse1krqf.org. 3600 IN NSEC3 1 1 0 332539EE7F95C32A 75U4T5QDUA8DUFCDA7PB5HRA87F07G6N NS DS RRSIG
75u43m27modtpregu0d0merldse1krqf.org. 3600 IN RRSIG NSEC3 8 2 3600 20250516152702 20250425142702 48111 org. ccvO2HviF/p/JIlqGMCnz93pJWzH8QiMqkCymi6jzOhpxDGDxB3J5aIZ V0
23xaPZzg5aAu1FPaLDlfzH4UOqIBcE8uX8bHI4sA8HDFlwTdh5aN6z zk5LSNSfmq107tKI6vkICFtjlswfogKJp8TP/CN9Fb4oU6WaxMmmBQ0V IRE=
;; Received 727 bytes from 199.19.57.1#53(d0.org.afilias-nst.org) in 36 ms

www.gnu.org.            1800    IN      A       209.51.188.116
gnu.org.                1800    IN      NS      ns2.gnu.org.
gnu.org.                1800    IN      NS      ns1.gnu.org.
gnu.org.                1800    IN      NS      ns4.gnu.org.
;; Received 270 bytes from 192.99.37.66#53(ns1.gnu.org) in 203 ms
```

Trazando DNS con Wireshark

1. ¿Qué protocolo de capa de transporte es usado en los mensajes DNS?

El protocolo de capa de transporte es UDP

2. ¿Cuál es el puerto origen y destino para la consulta DNS y su correspondiente respuesta?

El puerto de origen o Source es el: 3740 y el de destino o Destination es el: 52

3. ¿A qué dirección IP es enviada la consulta DNS? ¿Es la misma que el servidor DNS local por default?

Es enviado a la dirección 128.238.29.22, no el servidor por defecto es 192.168.100.1

4. ¿Cuántas preguntas están contenidas en el mensaje de consulta DNS? ¿Qué tipo (type) de consultas DNS son? ¿Puede que el mensaje de consulta tambien contenga alguna respuesta (answers)?

Se ve en la sección Questions que el valor es 1 y en las cuero consulta lo siguiente:

22.29.238.128.in-addr.arpa: type PTR, class IN

luego el siguiente mensaje marca el campo Answers

el PTR es 12, domain name pointer y la respuesta es el nombre del dominio dns-prime.poly.edu

5. Examine el mensaje de respuesta DNS. Exhiba los detalles del contenido de los campos "answers", "authority" y "additional information". ¿Qué puede concluir de los mismos?

lo que podemos concluir es que el mensaje tendrá una respuesta, que de hecho la tiene y es enviada, que no tiene nada adicional ni marca que es el servidor principal

6. ¿A qué dirección IP es enviada la consulta DNS? ¿Es la misma que el servidor DNS local por default?

Fue enviado a la direccion de IP 128.238.29.22, que no es la misma que la del DNS local

7. Examine el mensaje de consulta DNS ¿Qué tipo (type) de consultas DNS son? ¿Puede que el mensaje de consulta tambien contenga alguna respuesta (answers)?

El mensaje es de tipo NS, el mensaje contiene tres respuestas de:

bitsy.mit.edu

strawb.mit.edu

w20ns.mir.edu

8. Examine el mensaje de respuesta DNS. Exhiba los detalles del contenido de los campos "answers", "authority" y "additional information". ¿Qué puede concluir de los mismos?

en el caso del último paquete, podemos ver que en answers enumera la cantidad de respuestas y additional da más información sobre los mismos, en este caso las direcciones ip