

TRABAJO PRACTICO DNS

Administración de Redes Locales

Trabajo de:
Benicio Sánchez Mandato

Link GitHub:
[GitHub](#)

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.gnu.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7200
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.gnu.org.                IN      A

;; ANSWER SECTION:
www.gnu.org.                1520    IN      A      209.51.188.116

;; Query time: 268 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 19:31:25 -03 2025
;; MSG SIZE rcvd: 56
```

Figure 1: dig www.gnu.org

1 Comando DIG

1.1 Ejecutamos los comandos

Primero ejecutamos los comandos que manda ahí en el TP dando como resultado las siguientes respuestas:

En la próxima sección y respondiendo las Cuestiones analizaremos la información brindada por estos comandos.

```

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> gnu.org NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25852
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; 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: 176 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 19:34:52 -03 2025
;; MSG SIZE rcvd: 90

```

Figure 2: dig gnu.org NS

```

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> +trace www.gnu.org
;; global options: +cmd
.      150613 IN      NS      b.root-servers.net.
.      150613 IN      NS      j.root-servers.net.
.      150613 IN      NS      e.root-servers.net.
.      150613 IN      NS      a.root-servers.net.
.      150613 IN      NS      n.root-servers.net.
.      150613 IN      NS      d.root-servers.net.
.      150613 IN      NS      h.root-servers.net.
.      150613 IN      NS      f.root-servers.net.
.      150613 IN      NS      g.root-servers.net.
.      150613 IN      NS      i.root-servers.net.
.      150613 IN      NS      c.root-servers.net.
.      150613 IN      NS      l.root-servers.net.
.      150613 IN      NS      k.root-servers.net.
;; Received 811 bytes from 127.0.0.53#53(127.0.0.53) in 13 ms

org.      172800 IN      NS      a0.org.afilias-nst.info.
org.      172800 IN      NS      a2.org.afilias-nst.info.
org.      172800 IN      NS      b0.org.afilias-nst.org.
org.      172800 IN      NS      b2.org.afilias-nst.org.
org.      172800 IN      NS      c0.org.afilias-nst.info.
org.      172800 IN      NS      d0.org.afilias-nst.org.
org.      86400  IN      DS      26974 8 2 4FEDE294C53F438A158C41D39489CD78A86BEB0D8A0AEAFF14745C0D 16E1D
E32
org.      86400  IN      RRSIG   DS 8 1 86400 20250916170000 20250903160000 46441 . SFnJskMBpbcF8S1tLMcG
3AbwvYAGtmUMXs3lu2NXQ6ZALVUxeYd4lSc ZQyA3okfFLSoh5gB15b0AAg0CxutC60Mx30zUFnbRLQ4ap0JzZPNen63 GBqjh80g5olbz7LXI6p+q+65HML
fbheDMft6wEr0iIe1J13hkNUJod3A sSPGzP2U9tjecxsQpuUjp7mU09fvBuxzg2KwD5P+lrkk55xTJ4u/3FM/ DPOPt4N/qSWHFxgdXmkrge2ghEuaMIRSE
PggzgVAr1TihwAPPp/StBKb fal0YL+nLooRQaIAFnWnl9uvDxjtgQJvEvo+4a+a70BToCqzTolZTgv 0NIJuw==

```

Figure 3: dig +trace www.gnu.org primera mitad

```
;; Received 777 bytes from 199.7.91.13#53(d.root-servers.net) in 149 ms

;; UDP setup with 2001:500:e::1#53(2001:500:e::1) for www.gnu.org failed: network unreachable.
;; no servers could be reached
;; UDP setup with 2001:500:e::1#53(2001:500:e::1) for www.gnu.org failed: network unreachable.
;; no servers could be reached
;; UDP setup with 2001:500:e::1#53(2001:500:e::1) for www.gnu.org failed: network unreachable.
;; UDP setup with 2001:500:b::1#53(2001:500:b::1) for www.gnu.org failed: network unreachable.
;; UDP setup with 2001:500:48::1#53(2001:500:48::1) for www.gnu.org failed: network unreachable.
gnu.org.          3600    IN      NS      ns2.gnu.org.
gnu.org.          3600    IN      NS      ns1.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 20250924223527 20250903213527 14268 org. kRxKJCBEfaPK
YFbGgW16QvevRtBv4A7WxD+dEBs6DpHfMsrtLRzhJsgJ jwHq6T6m8He1YHJaDmqwL8I1fbTmSOVn2dzSJlCoHymysU2IwSBgvx5c j6Bmliqrze0+AZHg7u
7HdcPjrkqn58F/qIFGMjpAw00JDJqyJgc8QmIP 7C0=
75u43n27modtpregu0d0merldse1krqf.org. 3600 IN NSEC3 1 1 0 332539EE7F95C32A 75U4T5QDUa8DUFCDA7PB5HRA87F07G6N NS DS RRSIG
75u43n27modtpregu0d0merldse1krqf.org. 3600 IN RRSIG NSEC3 8 2 3600 20250922152719 20250901142719 14268 org. UNVz1GDZIQc0
B15m5CKODIXpQKBivtNkBiWiEb6X8NbwKt0pKgYNY3dh H7ybExtqdS0m49inQ3sj8Jg8iMzZy9bBPVYf3r8q5HAYY/rqS6fMOT1l i3knty36f7PhHScVt/
+rPBVUQTejIFxKz0SpUpb0p6H1NFFoYt+1x/0n qnE=
;; Received 727 bytes from 199.19.56.1#53(a0.org.afillias-nst.info) in 35 ms

www.gnu.org.      1800    IN      A       209.51.188.116
gnu.org.          1800    IN      NS      ns1.gnu.org.
gnu.org.          1800    IN      NS      ns2.gnu.org.
gnu.org.          1800    IN      NS      ns4.gnu.org.
;; Received 270 bytes from 188.165.235.157#53(ns4.gnu.org) in 222 ms
```

Figure 4: dig +trace www.gnu.org segunda mitad

1.2 Cuestiones

1.2.1 Pregunta 1

El nombre canonico de GNU es www.gnu.org y su direccion ip es 209.51.188.116,esto lo vemos en la primer imagen en la parte de ANSWER SECTION.

1.2.2 Pregunta 2

En el resto de la respuesta vemos IN que quiere decir que pertenece a internet la información y 367 que es el tiempo de vida de esta entrada lo que quiere decir que esta información es volátil debido a lo bajo de este valor.

1.2.3 Pregunta 3

La dirección ip del servidor DNS que responde la consulta es 127.0.0.53,este servidor es el servidor root que de forma recursiva le pregunta al resto luego por el org y por el gnu,esta información la sacamos de la primer imagen en la parte SERVER.

1.2.4 Pregunta 4

Tener un alias de este servidor DNS es importante para poder ubicarlo,de forma mas sencilla entre todos los que hay ya que cada uno de estos servidores por el mundo se identifican con una letra inicial distinta y todos estos servidores se

engloban dentro de una misma ip asi al iniciar la comunicación se pone esa ip y listo y se hacen la consulta a todos los NS disponible,la lista de todos los NS de este server lo vemos en la primer parte de la tercer foto,vemos que se listan 13 servidores.

1.2.5 Pregunta 5

Para gnu.org hay tres NS,los cuales se ven en la segunda imagen

- ns1.gnu.org
- ns2.gnu.org
- ns4.gnu.org

Luego poniendo el comando dig,sobre cada NS,vamos averiguando sus ip

- ns1.gnu.org → 192.99.37.66
- ns2.gnu.org → 192.99.35.98
- ns4.gnu.org → 188.165.235.157

Si vamos a la pagina whois.com vemos que la lista de NS es exactamente la que marcamos recién,confirmando la información,este acceso lo vemos en la imagen 5.

gnu.org Updated 3 days ago ↻

Domain Information	
Domain:	gnu.org
Registered On:	1995-11-24
Expires On:	2025-11-23
Updated On:	2025-04-28
Status:	client transfer prohibited
Name Servers:	ns4.gnu.org ns1.gnu.org ns2.gnu.org

Figure 5: Busqueda en whois.com

Constatar esta información está bueno para confirmar que existen estos tres NS y que se pueden utilizar de manera confiable.

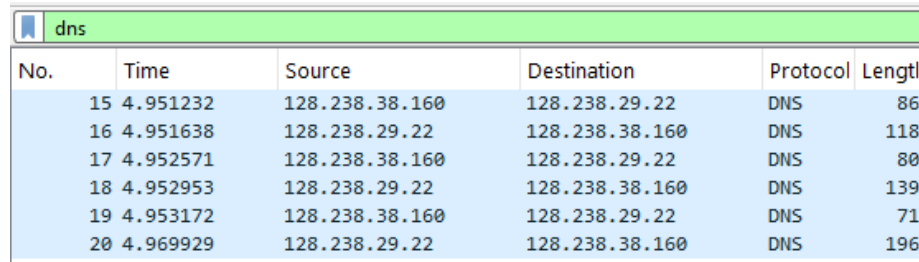
1.2.6 Pregunta 6

Ejecutando el comando, dig +trace www.gnu.org, obtuvimos los NS de los root-servers, de los servers para org, de los para gnu.org y la ip es www.gnu.org además vemos que se utiliza el protocolo de transporte UDP, todo esto está reflejado en las imágenes 3 y 4 vistas más arriba

2 WireShark

2.1 Primer Trama

Al abrir la primer trame y filtrar los DNS nos quedamos con seis eventos que los vemos en la imagen 6



No.	Time	Source	Destination	Protocol	Length
15	4.951232	128.238.38.160	128.238.29.22	DNS	86
16	4.951638	128.238.29.22	128.238.38.160	DNS	118
17	4.952571	128.238.38.160	128.238.29.22	DNS	80
18	4.952953	128.238.29.22	128.238.38.160	DNS	139
19	4.953172	128.238.38.160	128.238.29.22	DNS	71
20	4.969929	128.238.29.22	128.238.38.160	DNS	196

Figure 6: Eventos Primer Trama

Como dice el TP vamos a centrarnos en los últimos dos eventos de los cuales sacamos la siguiente información, que se analizara en las siguientes preguntas.

```

> Frame 19: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3742, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
\[Response In: 20\]

```

Figure 7: Primer Trama - Penúltimo Evento

2.1.1 Pregunta 1

DNS utiliza el protocolo de capa de transporte UDP, esto lo vemos en la Imagen 7 donde dice User Datagram Protocol es el protocolo de transporte en el que esta encapsulado.

2.1.2 Pregunta 2

El puerto origen de la consulta DNS es 3742 y el destino es 53 en la respuesta será viceversa origen 53 destino 3742, esto se ve en la misma parte que lo de la pregunta 1.

2.1.3 Pregunta 3

El paquete DNS es enviado a la dirección 128.238.29.22, como se ve en el destination del penúltimo paquete, esta es la del servidor por defecto según lo dicho en las consignas.

2.1.4 Pregunta 4

Hay contenido una pregunta en el mensaje de consulta DNS, la pregunta es de tipo A (host Address), en este caso el campo no contiene ninguna respuesta pero vemos que están dadas las condiciones ya que hay una línea de Answers RRs que en este caso está en 0 o sea que no contiene respuestas, todo esto se ve en la Imagen 7.

2.1.5 Pregunta 5

En el mensaje de respuesta vemos un Answer que contiene la dirección ip de www.mit.edu que en este caso es 18.7.22.83. Además vemos los nombres de los

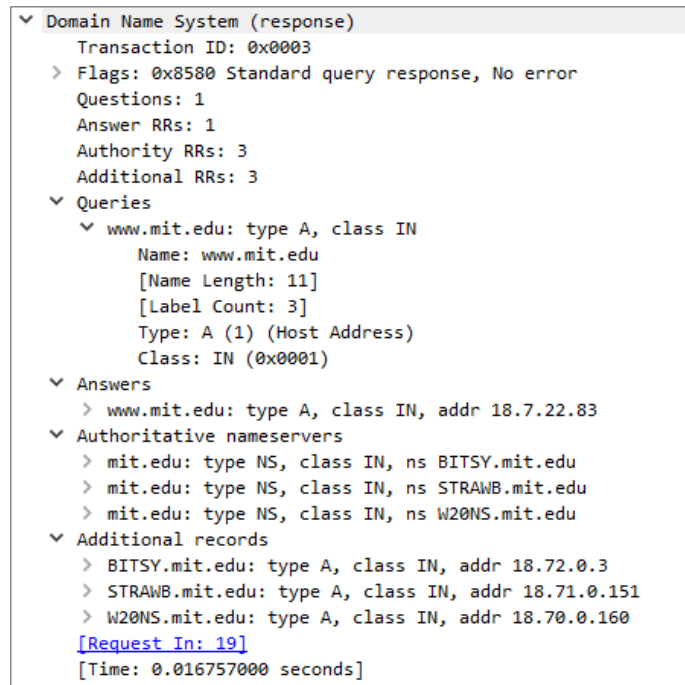


Figure 8: Primer Trama - Último Evento

NS que tiene el mit.edu, esto en el campo Authoritative nameservers los cuales son tres:

- BITSY.mit.edu
- STRAWB.mit.edu
- W20NS.mit.edu

Y por último en Additional records vemos las direcciones ip de estos tres NS. Estas Son:

- BITSY.mit.edu → 18.72.0.3
- STRAWB.mit.edu → 18.71.0.151
- W20NS.mit.edu → 18.70.0.160

Toda esta información se ve de forma clara en la Imagen 8.

2.2 Segunda Trama

En esta segunda trama filtrando en DNS vemos seis eventos, misma cantidad que en trama previa. El trabajo también nos pide analizar las últimas dos tramas de las cuales sacamos la información vista en Imágenes 10 y 11 que analizaremos en las preguntas.

dns					
No.	Time	Source	Destination	Protocol	Length
488	30.916492	128.238.38.160	128.238.29.22	DNS	86
489	30.916859	128.238.29.22	128.238.38.160	DNS	118
490	30.917700	128.238.38.160	128.238.29.22	DNS	76
491	30.918044	128.238.29.22	128.238.38.160	DNS	135
492	30.918275	128.238.38.160	128.238.29.22	DNS	67
493	30.918636	128.238.29.22	128.238.38.160	DNS	176

Figure 9: Eventos Segunda Trama

```

> Frame 492: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.22
> User Datagram Protocol, Src Port: 3746, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0003
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    ....0. .... = Truncated: Message is not truncated
    ....1. .... = Recursion desired: Do query recursively
    ....0.. .... = Z: reserved (0)
    .......0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
\[Response In: 493\]

```

Figure 10: Segunda Trama - Penúltimo Evento

```

> Internet Protocol Version 4, Src: 128.238.29.22, Dst: 128.238.38.160
> User Datagram Protocol, Src Port: 53, Dst Port: 3746
▼ Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 3
  ▼ Queries
    ▼ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
  ▼ Answers
    > mit.edu: type NS, class IN, ns bitsy.mit.edu
    > mit.edu: type NS, class IN, ns strawb.mit.edu
    > mit.edu: type NS, class IN, ns w20ns.mit.edu
  ▼ Additional records
    > bitsy.mit.edu: type A, class IN, addr 18.72.0.3
    > strawb.mit.edu: type A, class IN, addr 18.71.0.151
    > w20ns.mit.edu: type A, class IN, addr 18.70.0.160
\[Request In: 492\]
[Time: 0.000361000 seconds]

```

Figure 11: Segunda Trama - Último Evento

2.2.1 Pregunta 6

La consulta DNS es enviada a la dirección 128.238.29.22 que es la misma que el servidor local por default,esto se ve en la Imagen 9

2.2.2 Pregunta 7

Ahora hay otra vez una pregunta en esta consulta pero esta vez es de tipo 2 (NS) por lo cual está preguntando por el NS y no por la dirección ip como en el caso anterior,también vemos que el mensaje otra vez puede contener respuestas pero en este caso no las contiene,esto lo vemos en la Imagen 10.

2.2.3 Pregunta 8

Vemos que hay respuestas en este caso tres que son los tres NS que mencionamos anteriormente en la consigna 5,también en adicional hay tres respuestas que son las tres direcciones ip mencionadas también la consigna 5,lo que no hay es campo authority ya que en este caso eso se contesta en la misma respuesta ya que es la pregunta a responder,esto lo vemos en la Imagen 11

2.3 Comando nslookup

Ejecutando el comando, `nslookup -sil -type=NS mit.edu`, nos encontramos con sorpresas:

```
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = ns1-37.akam.net.

Authoritative answers can be found from:
asia2.akam.net  internet address = 95.101.36.64
asia1.akam.net  internet address = 95.100.175.64
eur5.akam.net   internet address = 23.74.25.64
```

Figure 12: comando `nslookup -sil -type=NS mit.edu`

Lo más notorio es que los NS listados no coinciden con los vistos en las preguntas, esto se puede atribuir al paso del tiempo capaz desde el armado de la trama a la actualidad hubo un cambio en estos, creandose nuevos y renombrando los anteriores, también vemos que el servidor DNS no coincide con el dado en la trama aunque eso puede deberse más a que quizá en la terminal nos indica otro servidor.

Lo importante de esto es que vemos como el DNS cambia a través del tiempo sufriendo modificaciones en sus NS, Ips, entre otras cosas, pero el principal DNS, que es mit.edu en este caso, no ha cambiado por lo que estos cambios no afectan en sí a los usuarios si no es más una cuestión interna.