

# Network Administration/System Administration (NTU CSIE, Spring 2024)

## Homework #7

B12902110 呂承諺

April 7, 2024

### 1 Do you know what is DNS?

1. DNS stands for Domain Name System. It is a naming system for hosts and services in the Internet. It manages various information associated with a domain name, such as its IP address, aliases, name servers, etc.

#### References

- [Domain Name System - Wikipedia](#)
- [Dynamic DNS | Cloudflare](#)

2. DDNS stands for Dyanmic DNS. It is a service that that automatically updates DNS records when an IP address of the service or resource changes.

#### References

- [Dynamic DNS | Cloudflare](#)

3. There are 13 root name servers.

#### References

- [Root name server - Wikipedia](#)

4. An example is the Sender Policy Framework (SPF). It list all the servers that are authorized to send email messages from a domain. Email receivers can then compare the SPF information with the email's header to confirm the email is sent from a reliable source. This is needed because SMTP allows any computer to send email claiming to be any source address, which could lead to spamming or phishing.

#### References

- [Sender Policy Framework - Wikipedia](#)
- [What is a DNS TXT record? | Cloudflare](#)

## 2 Do you know how to reach CSIE DNS?

```
$ dig +trace -4 www.csie.ntu.edu.tw
```

```
b12902110@ws1: ~  
$ dig +trace -4 www.csie.ntu.edu.tw  
  
; <<>> DiG 9.18.25 <<>> +trace -4 www.csie.ntu.edu.tw  
;; global options: +cmd  
.                46738    IN      NS      f.root-servers.net.  
.                46738    IN      NS      l.root-servers.net.  
.                46738    IN      NS      e.root-servers.net.  
.                46738    IN      NS      j.root-servers.net.  
.                46738    IN      NS      b.root-servers.net.  
.                46738    IN      NS      h.root-servers.net.  
.                46738    IN      NS      m.root-servers.net.  
.                46738    IN      NS      d.root-servers.net.  
.                46738    IN      NS      g.root-servers.net.  
.                46738    IN      NS      c.root-servers.net.  
.                46738    IN      NS      k.root-servers.net.  
.                46738    IN      NS      a.root-servers.net.  
.                46738    IN      NS      i.root-servers.net.  
.                46738    IN      RRSIG   NS 8 0 518400 2024041917  
F+ZDE760VRN2RvEGW4b8DudiTunmqPIe9d8z8c4uQ S9MHD5+cas+ipUK9v3rFD86rZGNQG0  
geSfFeWhvmtHn3twrtX0yBHHzfJAFWCWQLM3CYJbL9 z+eUwEJ0Ph1FDiv0vsa67jeRe1ZW37  
;; Received 525 bytes from 10.217.44.1#53(10.217.44.1) in 0 ms  
  
tw.              172800   IN      NS      a.dns.tw.  
tw.              172800   IN      NS      b.dns.tw.  
tw.              172800   IN      NS      c.dns.tw.  
tw.              172800   IN      NS      d.dns.tw.  
tw.              172800   IN      NS      e.dns.tw.  
tw.              172800   IN      NS      f.dns.tw.  
tw.              172800   IN      NS      g.dns.tw.  
tw.              172800   IN      NS      h.dns.tw.  
tw.              172800   IN      NS      anytld.apnic.net.  
tw.              86400    IN      DS      51277 8 2 462DA9AF501D2B  
tw.              86400    IN      RRSIG   DS 8 1 86400 20240420050  
p44ckvH9m14Dig07G2y4TqmwrpFL1AU5rwjkNmbz hCqQcxd3GpXyaCny9TLY0UGeTluKm1/  
W0V+Zh/a7zF8PKkkpYRbxha1Qncb3d0u5YqAYmWn s91cFW26MZSvyB1Levy7w1RQjeHC3yK  
;; Received 885 bytes from 199.7.91.13#53(d.root-servers.net) in 30 ms
```

```

edu.tw. 3600 IN NS moestar.edu.tw.
edu.tw. 3600 IN NS c.twnic.net.tw.
edu.tw. 3600 IN NS a.twnic.net.tw.
edu.tw. 3600 IN NS edudns-a3.edu.tw.
edu.tw. 3600 IN NS moemoon.edu.tw.
edu.tw. 3600 IN NS edudns-a1.edu.tw.
edu.tw. 3600 IN NS d.twnic.net.tw.
edu.tw. 3600 IN NS b.twnic.net.tw.
edu.tw. 3600 IN NS edudns-a2.edu.tw.
edu.tw. 300 IN DS 11734 8 2 EF2A91584B1949B95F
edu.tw. 300 IN DS 24025 8 2 7DFE1D2793B0905653
edu.tw. 300 IN DS 54865 8 2 7F238ADB803F363C3D
edu.tw. 300 IN RRSIG DS 8 2 300 20240507080022 26
+uRHOG/N37yae3KRhvgtxF5yHkAbPVkNRVgPzGfDt MapEW4oWmIoGcxrZvzf+bCn5BFfUgJa58c
;; Received 968 bytes from 204.61.216.119#53(h.dns.tw) in 30 ms

ntu.edu.tw. 300 IN NS dns.tp1rc.edu.tw.
ntu.edu.tw. 300 IN NS dns.ntu.edu.tw.
ntu.edu.tw. 300 IN NS ntu3.ntu.edu.tw.
CFHNKGNQ5QOBIB61FV5AKT0CR5554JKT.edu.tw. 300 IN NSEC3 1 0 10 5B7A95B3E7E6DD6
CFHNKGNQ5QOBIB61FV5AKT0CR5554JKT.edu.tw. 300 IN RRSIG NSEC3 8 3 300 20240416
QtplFhkF4BAAXNIZFoYofNuBCi6076qUqUo69z0t9maHhCk71AjUa TPoISDUfXnTIXLXhsaqvS
;; Received 433 bytes from 211.73.64.22#53(a.twnic.net.tw) in 3 ms

csie.ntu.edu.tw. 14400 IN NS csman.csie.ntu.edu.tw.
csie.ntu.edu.tw. 14400 IN NS csman2.csie.ntu.edu.tw.
;; Received 121 bytes from 163.28.16.10#53(dns.tp1rc.edu.tw) in 0 ms

www.csie.ntu.edu.tw. 600 IN A 140.112.30.26
www.csie.ntu.edu.tw. 600 IN RRSIG A 7 5 600 20240426061133 202
mRe+hcRpmkDgAcEHtZAAeXzSkPbDgeTaoFKRbWLH2+1i2Ly2Is9vp d06qvt1HE8j1C9ibon9ei0
2PRk2eMBalyn8umjD+NXi4tKODWgAjGR2kYbgM5huHTLfMKNuW4yK w/b6wKq8To4VLucLtt6+cv
csie.ntu.edu.tw. 600 IN NS ntuns.ntu.edu.tw.
csie.ntu.edu.tw. 600 IN NS csman.csie.ntu.edu.tw.
csie.ntu.edu.tw. 600 IN NS csman2.csie.ntu.edu.tw.
csie.ntu.edu.tw. 600 IN RRSIG NS 7 4 600 20240426061133 26
N3YqQ2xjre7SbLCpvpb83tPIkypf4LPYILdSEa8Js67jbzFaEl6Zkqf YMqJ9MhcTh2VjckVyMCLB
1+qZ3a5xjVpG+xNh8p8w5GaaJY5F69zAzidK4d1fVU0rGf4VB/QEFY cpSSigWPDbhNW0fD/3uzC
;; Received 1066 bytes from 140.112.30.13#53(csman.csie.ntu.edu.tw) in 3 ms

```

Domain Name	IP address	Zone
d.root-servers.net	199.7.91.13	Root
h.dns.tw	204.61.216.119	tw
a.twnic.net.tw	211.73.64.22	edu.tw
dns.tp1rc.edu.tw	163.28.16.10	ntu.edu.tw
csman.csie.ntu.edu.tw	140.112.30.13	csie.ntu.edu.tw
www.csie.ntu.edu.tw	140.112.30.26	N/A

## References

- [dns - How does dig +trace actually work? - Super User](#)

### 3 Do you know how to design a DNS architecture?

- Basic DNS server setup:
  - Setup a DNS server, preferably with a static IP address `xxx.xxx.xxx.xxx`.
  - Register the following records to the authoritative servers of zone `ntu.edu.tw`.  
(Zone: `ntu.edu.tw`)

Name	Type	Data
<code>csie</code>	NS	<code>ns.csie.ntu.edu.tw.</code>
<code>ns.csie</code>	A	<code>xxx.xxx.xxx.xxx</code>

- Q : 如果今天其中一台伺服器壞掉了怎麼辦？

A : Maintain multiple mirror servers, and register multiple NS and A records to the authoritative servers of zone `ntu.edu.tw`.

(Zone: `ntu.edu.tw`)

Name	Type	Data
<code>csie</code>	NS	<code>ns1.csie.ntu.edu.tw.</code>
<code>csie</code>	NS	<code>ns2.csie.ntu.edu.tw.</code>
<code>csie</code>	NS	<code>ns3.csie.ntu.edu.tw.</code>
<code>ns1.csie</code>	A	<code>xxx.xxx.xxx.xxx</code>
<code>ns2.csie</code>	A	<code>yyy.yyy.yyy.yyy</code>
<code>ns3.csie</code>	A	<code>zzz.zzz.zzz.zzz</code>

- Q : 如果今天系館停電導致所有機房下線怎麼辦？

A : Place at least one of the CSIE DNS servers elsewhere, such as in 計中 or outside of NTU.

- Q : 如果因為某些原因導致伺服器上的 DNS records 不見了怎麼辦？

A :

- Regularly backup all configurations, including DNS records.
- Keep a log of all configuration changes.

- Q : 有些實驗室想要擁有自己的 subdomain，該如何實現？

A : Register NS and A records of the lab's DNS server to our DNS server.

(Zone: `csie.ntu.edu.tw`)

Name	Type	Data
<code>lab1</code>	NS	<code>ns.lab1.csie.ntu.edu.tw.</code>
<code>ns.lab1</code>	A	<code>xxx.xxx.xxx.xxx</code>
<code>lab2</code>	NS	<code>ns.lab2.csie.ntu.edu.tw.</code>
<code>ns.lab2</code>	A	<code>yyy.yyy.yyy.yyy</code>

- Q：如何應對 DNS flooding attack？

A：

- Limit the rate of queries from a single source.
- Limit repeated queries for nonexistent domains.
- Distribute DNS service across multiple servers.

- Q：如何應對 DNS amplification attack？

A：

- Limit the rate of queries from a single source.
- Only provide service to the necessary networks.
- Reject traffic sent with the spoofed IP addresses.

- Q：如何確保對 \*.csie.ntu.edu.tw 的 query response 不會被攻擊者竄改成 malicious ip 呢？

A：Use DNSSEC or DNS over TLS.

## References

- [domain name system - Why don't NS records contain IP addresses? - Server Fault](#)
- [What is a DNS flood? | DNS flood DDoS attack | Cloudflare](#)
- [Understanding and Preventing DNS Flood Attacks](#)
- [DNS amplification DDoS attack | Cloudflare](#)

## 4 The Power of DNS

The operating system is Ubuntu 22.04.4 LTS. Assume that Docker is already installed and configured.

### 1. Steps

- (a) Install the required packages.

```
$ sudo apt-get install -y \
    mysql-server pdns-server pdns-backend-mysql
```

- (b) Run the following SQL commands:

```
$ sudo mysql
mysql> CREATE USER 'powerdns'@'localhost'
    -> IDENTIFIED BY 'powerdns-mysql-password';
Query OK, 0 rows affected (0.02 sec)
mysql> CREATE DATABASE powerdns;
Query OK, 1 row affected (0.20 sec)
mysql> GRANT ALL ON powerdns.* TO 'powerdns'@'localhost';
Query OK, 0 rows affected (0.16 sec)
mysql> exit
$ sudo mysql -u powerdns -p powerdns \
    < /usr/share/pdns-backend-mysql/schema/schema.mysql.sql
```

- (c) Change the following setting in `/etc/powerdns/pdns.conf`:

```
launch=gmysql
gmysql-password=powerdns-mysql-password
```

- (d) Free up 53 port for the PowerDNS server.

```
$ sudo systemctl stop systemd-resolved
```

- (e) (Re)start the PowerDNS server.

```
$ sudo systemctl restart pdns.service
```

## Result

```
user@ubuntu-vm1:/var/log/mysql$ systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-04-07 14:48:34 CST; 25min ago
     Process: 29406 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
    Main PID: 29414 (mysqld)
      Status: "Server is operational"
        Tasks: 42 (limit: 4595)
       Memory: 401.1M
          CPU: 14.394s
      CGroup: /system.slice/mysql.service
              └─29414 /usr/sbin/mysqld

[4] 07 14:48:33 ubuntu-vm1 systemd[1]: Starting MySQL Community Server...
[4] 07 14:48:34 ubuntu-vm1 systemd[1]: Started MySQL Community Server.

user@ubuntu-vm1:~$ systemctl status pdns.service
● pdns.service - PowerDNS Authoritative Server
   Loaded: loaded (/lib/systemd/system/pdns.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-04-07 13:29:06 CST; 34s ago
     Docs: man:pdns_server(1)
           man:pdns_control(1)
           https://doc.powerdns.com
    Main PID: 7418 (pdns_server)
      Tasks: 10 (limit: 4595)
       Memory: 42.8M
          CPU: 132ms
      CGroup: /system.slice/pdns.service
              └─7418 /usr/sbin/pdns_server --guardian=no --daemon=no --disable-syslog --log-timestamp=no --write-pid=no

[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: TCP server bound to 0.0.0.0:53
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: TCP server bound to [::]:53
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: PowerDNS Authoritative Server 4.5.3 (C) 2001-2021 PowerDNS.COM BV
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: Using 64-bits mode. Built using gcc 11.2.0.
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: PowerDNS comes with ABSOLUTELY NO WARRANTY. This is free software, and y
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: [webserver] Listening for HTTP requests on 127.0.0.1:8081
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: Creating backend connection for TCP
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: About to create 3 backend threads for UDP
[4] 07 13:29:06 ubuntu-vm1 systemd[1]: Started PowerDNS Authoritative Server.
[4] 07 13:29:06 ubuntu-vm1 pdns_server[7418]: Done launching threads, ready to distribute questions
```

## References

- [Installing PowerDNS —PowerDNS Authoritative Server documentation](#)
- [Debian – Package Search Results – pdns-backend](#)
- [解決 Ubuntu 上 53 Port 占用問題 | 小易的部落格](#)
- [Backends —PowerDNS Authoritative Server documentation](#)
- [Generic MySQL backend —PowerDNS Authoritative Server documentation](#)
- [Install and configure a MySQL server | Ubuntu](#)
- [sql - MySQL Error: : 'Access denied for user 'root'@'localhost' - Stack Overflow](#)
- [PowerDNS - hoyo 學習紀錄](#)

## 2. Steps

- (a) Change the following settings in `/etc/powerdns/pdns.conf`:

```
api=yes
api-key=b12902110-pdns-key
```

- (b) (Re)start the PowerDNS server.

```
$ sudo systemctl restart pdns.service
```

- (c) Verify that the PowerDNS API is configured properly:

```
$ curl -H 'X-API-Key: b12902110-pdns-key' \
  http://127.0.0.1:8081/api/v1/servers/localhost/zones
```

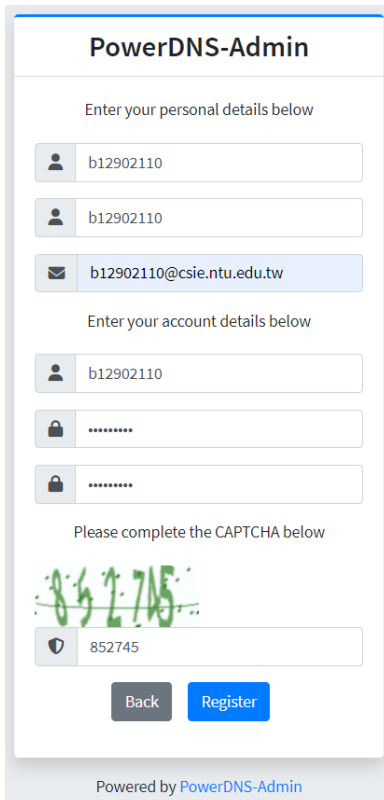
The output should be an empty array for now:

```
[]
```

- (d) Start the PowerDNS-Admin Docker container. Make sure to use host type network.

```
$ sudo docker run -d \
  -e SECRET_KEY='b12902110-flask-key' \
  -e BIND_ADDRESS=0.0.0.0:9191 \
  -v pda-data:/data \
  --network=host \
  powerdnsadmin/pda-legacy:latest
```

- (e) Go to the web interface of PowerDNS-Admin (<http://localhost:9191/>) and create an account.

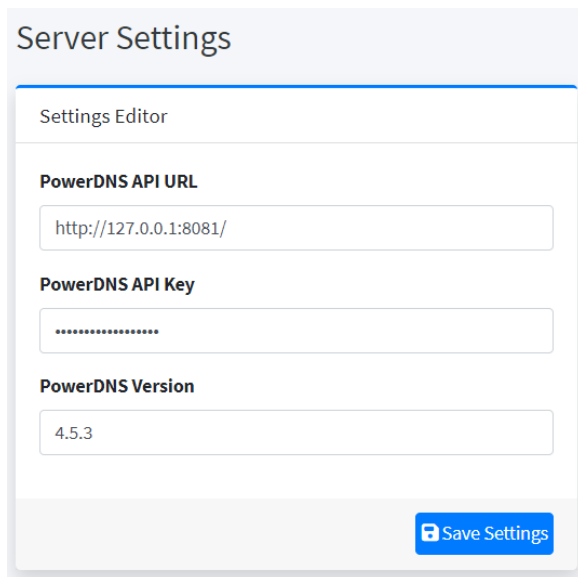


The screenshot shows the PowerDNS-Admin web interface. At the top, it says "PowerDNS-Admin". Below that, it prompts the user to "Enter your personal details below". There are three input fields: a username field with "b12902110", a password field with "b12902110", and an email field with "b12902110@csie.ntu.edu.tw". Below these, it prompts the user to "Enter your account details below". There are two more input fields: a username field with "b12902110" and a password field with "\*\*\*\*\*". Below these, it prompts the user to "Please complete the CAPTCHA below". There is a CAPTCHA image showing the number "852745" and a text input field with "852745". At the bottom, there are two buttons: "Back" and "Register". At the very bottom, it says "Powered by PowerDNS-Admin".



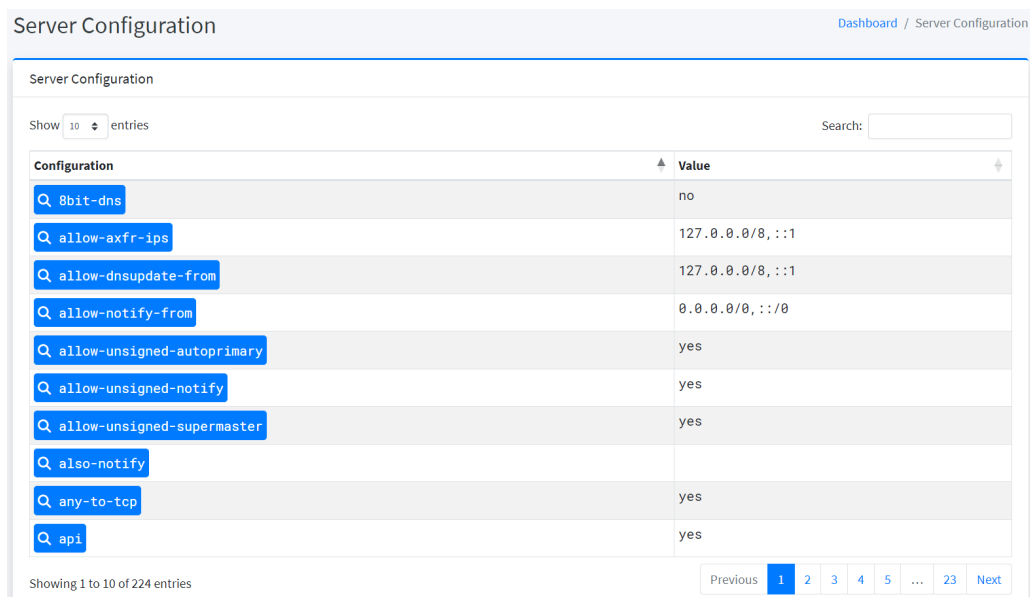
(f) Login and go to **Settings > Server**. Enter the following setting values:

- **PowerDNS API URL:** `http://127.0.0.1:8081/`
- **PowerDNS API Key:** `b12902110-pdns-key`
- **PowerDNS Version:** `4.5.3`



The screenshot shows the 'Server Settings' page in the PowerDNS Admin web interface. It features a 'Settings Editor' section with three input fields: 'PowerDNS API URL' containing 'http://127.0.0.1:8081/', 'PowerDNS API Key' with masked characters, and 'PowerDNS Version' containing '4.5.3'. A blue 'Save Settings' button is located at the bottom right of the form.

**Result** Go to **Server Configuration**. If the configurations show up, that means the API is configured successfully.



The screenshot shows the 'Server Configuration' page in the PowerDNS Admin web interface. It displays a table of configuration entries with a search bar and pagination controls. The table lists various configuration options and their values.

Configuration	Value
8bit-dns	no
allow-axfr-ips	127.0.0.0/8, ::1
allow-dnsupdate-from	127.0.0.0/8, ::1
allow-notify-from	0.0.0.0/0, ::/0
allow-unsigned-autoprimary	yes
allow-unsigned-notify	yes
allow-unsigned-supermaster	yes
also-notify	
any-to-tcp	yes
api	yes

## References

- [GitHub - PowerDNS-Admin/PowerDNS-Admin: A PowerDNS web interface with advanced features](#)
- [HTTP API - Introduction](#)
- [Built-in Webserver and HTTP API —PowerDNS Authoritative Server documentation](#)
- [PowerDNS-Admin/docs/wiki/configuration/Environment-variables.md at master · PowerDNS-Admin/PowerDNS-Admin · GitHub](#)

### 3. Steps

- (a) Go to **Create Zone** and create zone `nasa.csie.tw`.

Zone Editor

Zone Name

nasa.csie.tw

☐ Zone Override Record

Account

- No Account -

Zone Type

☒ Native

☐ Primary

☐ Secondary

Zone Template

No template

SOA-EDIT-API

☒ DEFAULT

☐ INCREASE

☐ EPOCH

☐ OFF

Cancel

Create Zone

- (b) Go to **Zone Records - nasa.csie.tw** and create the following records.

Name	Type	Data
*.sub	NS	subns.nasa.csie.tw.
subns	A	10.1.6.88
verification	TXT	"I LOVE NASA"

Zone Records - nasa.csie.tw

Dashboard / Zone Records - nasa.csie.tw

Zone Editor

Zone Settings








Changelog

+ Add Record

Save Changes

15 records

Search:

Name <sup>h</sup>	Type	Status	TTL	Data	Comment	Actions
*.sub	NS	Active	60	subns.nasa.csie.tw.		  
subns	A	Active	60	10.1.6.88		  
verification	TXT	Active	60	"I LOVE NASA"		

Showing 1 to 3 of 3 entries

Previous1Next

## Result

```
user@ubuntu-vm1:~$ dig @127.0.0.1 -t TXT verification.nasa.csie.tw

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @127.0.0.1 -t TXT verification.nasa.csie.tw
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46135
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;verification.nasa.csie.tw.      IN      TXT

;; ANSWER SECTION:
verification.nasa.csie.tw. 60      IN      TXT      "I LOVE NASA"

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Apr 07 15:58:58 CST 2024
;; MSG SIZE  rcvd: 78

user@ubuntu-vm1:~$ dig @127.0.0.1 *.sub.nasa.csie.tw

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @127.0.0.1 *.sub.nasa.csie.tw
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63534
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;*.sub.nasa.csie.tw.           IN      A

;; AUTHORITY SECTION:
*.sub.nasa.csie.tw. 60      IN      NS      subns.nasa.csie.tw.

;; ADDITIONAL SECTION:
subns.nasa.csie.tw. 60      IN      A      10.1.6.88

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Apr 07 16:01:15 CST 2024
;; MSG SIZE  rcvd: 83
```

## References

- [List of DNS record types - Wikipedia](#)
- [DNS NS record | Cloudflare](#)