

HW #2, Chapter 2

He Tianyang, 3022001441

October 5, 2024

Problem 1. Chapter 2 P 18

- (a) What is a whois database?
- (b) Use various whois databases on the Internet to obtain the names of two DNS servers. Indicate which whois databases you used.
- (c) Use `nslookup` on your local host to send DNS queries to three DNS servers: your local DNS server and the two DNS servers you found in part (b). Try querying for Type A, NS, and MX reports. Summarize your findings.
- (d) Use `nslookup` to find a Web server that has multiple IP addresses. Does the Web server of your institution (school or company) have multiple IP addresses?
- (e) Use the ARIN whois database to determine the IP address range used by your university.
- (f) Describe how an attacker can use whois databases and the `nslookup` tool to perform reconnaissance on an institution before launching an attack.
- (g) Discuss why whois databases should be publicly available.

Solutions:

a. What is a whois database?

A whois database is a publicly accessible resource that contains detailed information about domain names, IP address ranges, and autonomous systems. It is commonly used to look up information about the ownership of a domain name, the associated IP address range, and the autonomous system number (ASN).

b. Use various whois databases on the Internet to obtain the names of two DNS servers. Indicate which whois databases you used.

I used the ICANN WHOIS database to retrieve the DNS server information for google.com and facebook.com. The results are shown in Fig. 1 through Fig. 2, as well as in Tab. 1.

ICANN | LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

For additional information on ICANN Accredited Registrars including website and contact information, please visit <https://www.icann.org/en/accredited-registrars>.

If the registration data you are seeking is not provided in the lookup results, please use the [Registration Data Request Service \(RDRS\)](#) to submit a request for nonpublic registration data. RDRS is intended for use by requestors with a legitimate interest in accessing nonpublic registration data.

Domain Information

Name: GOOGLE.COM

Registry Domain ID: 2138514_DOMAIN_COM-VRSN

Domain Status:
[clientDeleteProhibited](#)
[clientTransferProhibited](#)
[clientUpdateProhibited](#)
[serverDeleteProhibited](#)
[serverTransferProhibited](#)
[serverUpdateProhibited](#)

Nameservers:
NS1.GOOGLE.COM
NS2.GOOGLE.COM
NS3.GOOGLE.COM
NS4.GOOGLE.COM

Dates

Registry Expiration: 2028-09-14 04:00:00 UTC

Updated: 2019-09-09 15:39:04 UTC

Created: 1997-09-15 04:00:00 UTC

Figure 1: ICANN WHOIS database result for google.com

c. Use nslookup on your local host to send DNS queries to three DNS servers: your local DNS server and the two DNS servers you found in part (b). Try querying for Type A, NS, and MX records. Summarize your findings.

To query DNS records for a target domain using nslookup, you can run the following command:

```
nslookup -type=<record_type> <domain> <dns_server,optional>
```

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

For additional information on ICANN Accredited Registrars including website and contact information, please visit <https://www.icann.org/en/accredited-registrars>.

If the registration data you are seeking is not provided in the lookup results, please use the [Registration Data Request Service \(RDRS\)](#) to submit a request for nonpublic registration data. RDRS is intended for use by requestors with a legitimate interest in accessing nonpublic registration data.

Domain Information

Name: FACEBOOK.COM

Registry Domain ID: 2320948_DOMAIN_COM-VRSN

Domain Status:

[clientDeleteProhibited](#)

[clientTransferProhibited](#)

[clientUpdateProhibited](#)

[serverDeleteProhibited](#)

[serverTransferProhibited](#)

[serverUpdateProhibited](#)

Nameservers:

A.NS.FACEBOOK.COM

B.NS.FACEBOOK.COM

C.NS.FACEBOOK.COM

D.NS.FACEBOOK.COM

Dates

Registry Expiration: 2033-03-30 04:00:00 UTC

Updated: 2024-04-24 19:06:12 UTC

Created: 1997-03-29 05:00:00 UTC

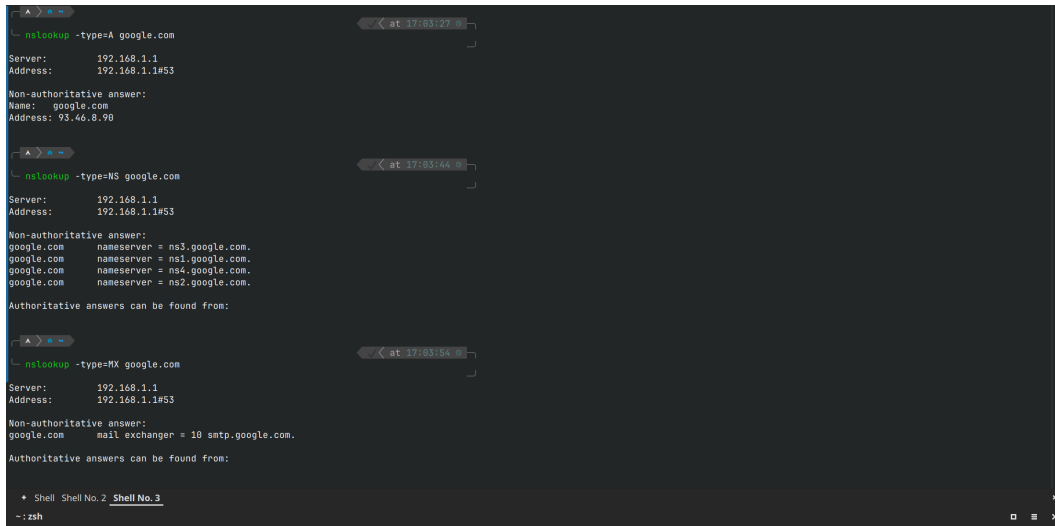
Figure 2: ARIN WHOIS database result for google.com

Domain	DNS Server
google.com	ns1.google.com
	ns2.google.com
	ns3.google.com
	ns4.google.com
facebook.com	a.ns.facebook.com
	b.ns.facebook.com
	c.ns.facebook.com
	d.ns.facebook.com

Table 1: DNS servers for google.com and facebook.com

First, we ran `nslookup` on the local DNS server. The results are displayed in Fig. 3.

```
nslookup -type=A google.com
nslookup -type=NS google.com
nslookup -type=MX google.com
```



```

nslookup -type=A google.com
Server:      192.168.1.1
Address:     192.168.1.1#53
Non-authoritative answer:
Name:   google.com
Address: 93.46.8.98

nslookup -type=NS google.com
Server:      192.168.1.1
Address:     192.168.1.1#53
Non-authoritative answer:
google.com  nameserver = ns3.google.com.
google.com  nameserver = ns1.google.com.
google.com  nameserver = ns4.google.com.
google.com  nameserver = ns2.google.com.
Authoritative answers can be found from:

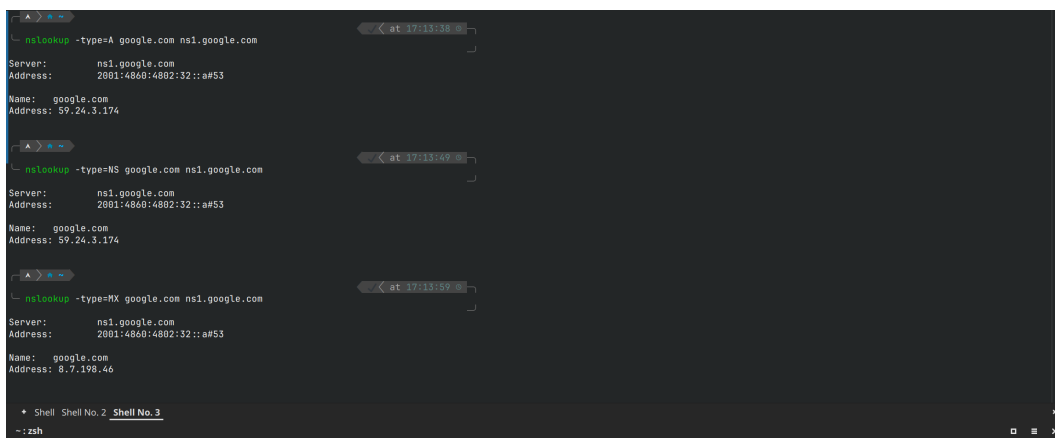
nslookup -type=MX google.com
Server:      192.168.1.1
Address:     192.168.1.1#53
Non-authoritative answer:
google.com  mail exchanger = 10 smtp.google.com.
Authoritative answers can be found from:

```

Figure 3: nslookup results for local DNS server

Second, we ran `nslookup` on `ns1.google.com`, and the results are shown in Fig. 4.

```
nslookup -type=A google.com ns1.google.com
nslookup -type=NS google.com ns1.google.com
nslookup -type=MX google.com ns1.google.com
```



```

nslookup -type=A google.com ns1.google.com
Server:      ns1.google.com
Address:     2001:4860:4802:32::a#53
Name:   google.com
Address: 59.24.3.174

nslookup -type=NS google.com ns1.google.com
Server:      ns1.google.com
Address:     2001:4860:4802:32::a#53
Name:   google.com
Address: 59.24.3.174

nslookup -type=MX google.com ns1.google.com
Server:      ns1.google.com
Address:     2001:4860:4802:32::a#53
Name:   google.com
Address: 8.7.198.46

```

Figure 4: nslookup results for ns1.google.com

Third, we ran `nslookup` on `ns2.google.com`, which is another DNS server for Google. The results are displayed in Fig. 5.

```
nslookup -type=A google.com ns2.google.com
```

```
nslookup -type=NS google.com ns2.google.com
nslookup -type=MX google.com ns2.google.com
```

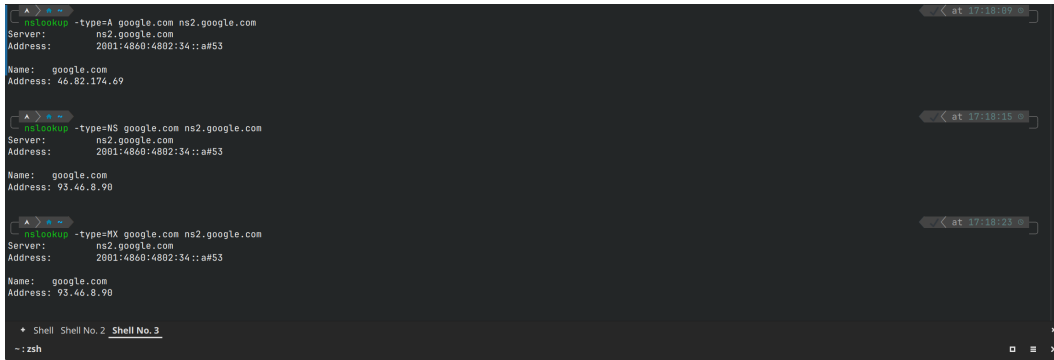


Figure 5: nslookup results for ns2.google.com

Now, let's inspect and summarize the results from the three DNS servers. The detailed results are presented in Tab. 2.

DNS Server	Type A	Type NS	Type MX
Local DNS	93.46.8.90	ns[1-4].google.com	smtp.google.com
ns1.google.com	59.24.3.174	59.24.3.174	8.7.198.46
ns2.google.com	46.82.174.69	93.46.8.90	93.46.8.90

Table 2: nslookup results for google.com

From the image and results, we can see that the local DNS server provides a ****Non-authoritative answer**** for all DNS records. This happens because the local DNS server is caching the results from the authoritative server.

Additionally, by examining the IP addresses in each report, we notice that the Type A records vary across different DNS servers. This is due to large websites like Google using multiple servers for load balancing and fault tolerance. Moreover, the Type NS records from 'ns2.google.com' match those of the local DNS server, further confirming that the local DNS server is caching results from the authoritative server.

d. Use nslookup to find a web server that has multiple IP addresses. Does your institution's web server (school or company) have multiple IP addresses?

Google is an example of a website with multiple IP addresses, as shown in Tab. 2.

Next, let's examine the official website of Tianjin University, <https://tju.edu.cn>, using Google's DNS server 8.8.8.8. The results are shown in Fig. 6.

```
nslookup -type=A tju.edu.cn 8.8.8.8
```



```

nslookup tju.edu.cn 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   tju.edu.cn
Address: 202.113.2.198
Name:   tju.edu.cn
Address: 2001:da8:a000:ab23::10

nslookup tju.edu.cn 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   tju.edu.cn
Address: 202.113.2.198
Name:   tju.edu.cn
Address: 2001:da8:a000:ab23::10

```

Figure 6: nslookup results for tju.edu.cn

Execute the command multiple times, it returns the same IP address which is 202.113.2.198. This indicates that the official website of Tianjin University does not have multiple IP addresses, which is reasonable because the server of the official website is at the same location in the campus and shares the same IPv4 Addresss.

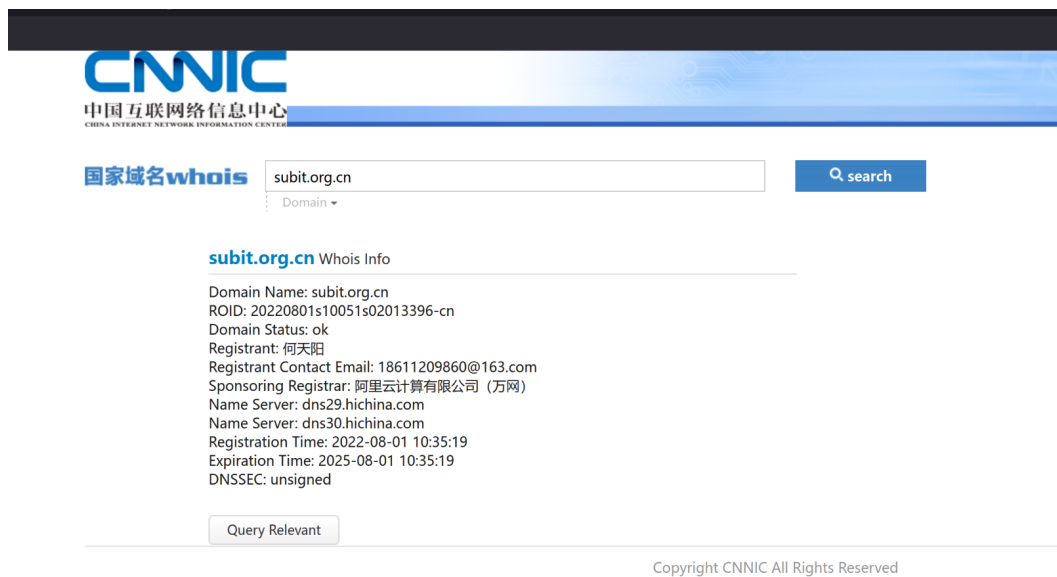
e. Use the ARIN whois database to determine the IP address range used by your university.

Tianjin University is located in Tianjin, China, and is registered through CERNET. Therefore, the ARIN whois database does not contain information about Tianjin University. Instead, we can use the CERNET whois database to find the IP address range used by Tianjin University. However, as of October 5, 2024, the CERNET whois database <https://web.nic.edu.cn/cgi-bin/reg/otherobj> is not available and returns Error Code 403, as shown in Fig. 7.



Figure 7: CERNET WHOIS database result for tju.edu.cn

Instead, Use CNNIC to check the whois information of subit.org.cn, which is my personal domain to show the process. The results are shown in Fig. 8.



CNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

国家域名whois

subit.org.cn
Domain

search

subit.org.cn Whois Info

Domain Name: subit.org.cn
ROID: 20220801s10051s02013396-cn
Domain Status: ok
Registrant: 何天阳
Registrant Contact Email: 18611209860@163.com
Sponsoring Registrar: 阿里云计算有限公司 (万网)
Name Server: dns29.hichina.com
Name Server: dns30.hichina.com
Registration Time: 2022-08-01 10:35:19
Expiration Time: 2025-08-01 10:35:19
DNSSEC: unsigned

Query Relevant

Copyright CNIC All Rights Reserved

Figure 8: CNIC WHOIS database result for subit.org.cn

f. Describe how an attacker can use whois databases and the nslookup tool to perform reconnaissance on an institution before launching an attack.

An attacker can use whois databases and the **nslookup** tool to gather valuable information about an institution's domain and network infrastructure. By querying a whois database, the attacker can retrieve details about the domain, such as the registrar, registration and expiration dates, nameservers, and sometimes even contact information for the domain owner or administrative staff. This data can help the attacker determine potential weak points, like outdated domain records or vulnerable domain management practices.

The **nslookup** tool allows attackers to perform DNS lookups on domain names or IP addresses. It can provide insights into the DNS records of the institution, including IP addresses linked to the domain, the type of DNS records in use (A, MX, CNAME, etc.), and the servers responsible for the domain's DNS resolution. By analyzing this information, the attacker can map the institution's network, identify possible entry points, or plan for DNS-related attacks like DNS spoofing or poisoning.

g. Discuss why whois databases should be publicly available.

Whois databases should be publicly available to promote transparency and accountability on the internet. By allowing access to information about domain ownership, individuals and organizations can verify the legitimacy of websites and domains, reducing the risk of online fraud or abuse. Public access to whois data can also assist in resolving domain-related disputes, such as intellectual property issues, as well as enabling law enforcement or security researchers to track down malicious entities responsible for cyberattacks or other illegal activities.

Moreover, public whois data facilitates network troubleshooting by providing essential details that can help administrators resolve issues related to domain misconfigurations or abuse. While privacy concerns exist, modern practices such as redacting sensitive contact information or using privacy protection services help strike a balance between transparency and personal privacy.