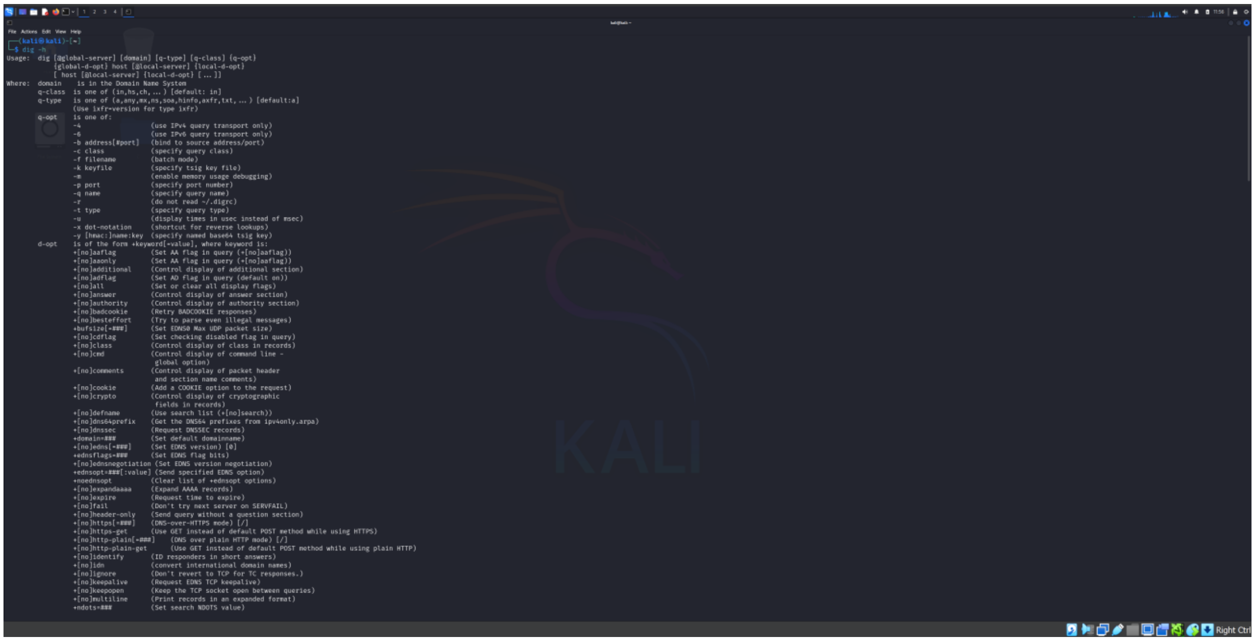
Lab 3

Demo Dig and Nslookup Tools

CSCI 4406_60L Computer Networks Lab

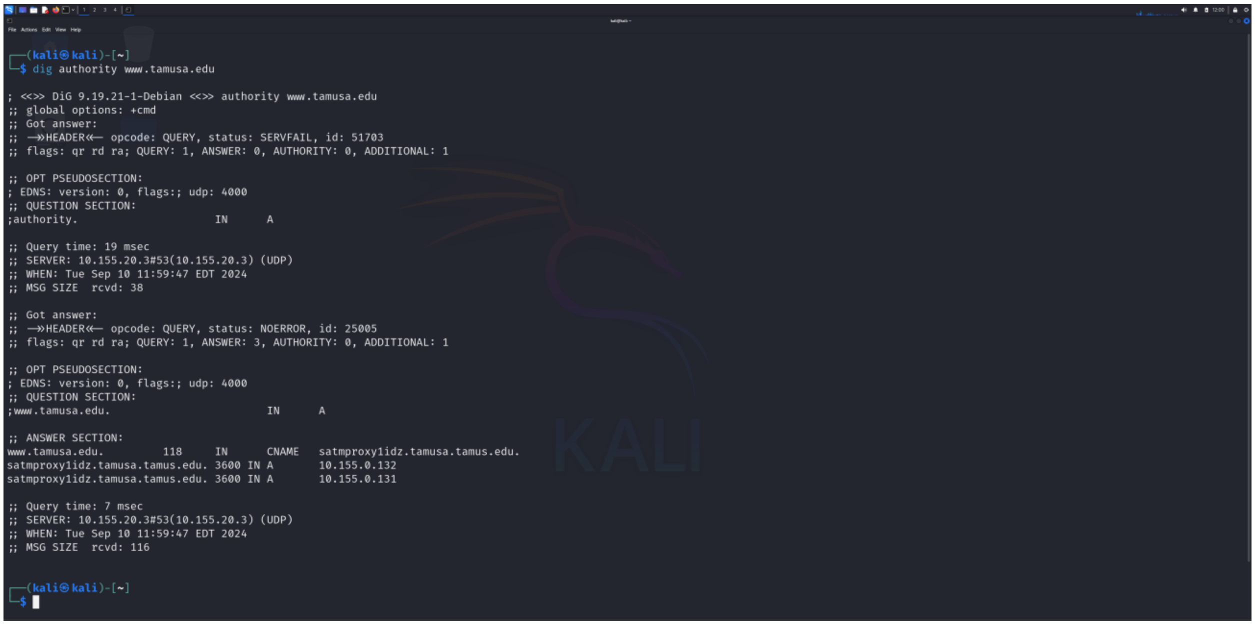
Joshua Ludolf

- I chose to use kali Linux and typed the dig help command to learn what it's for.



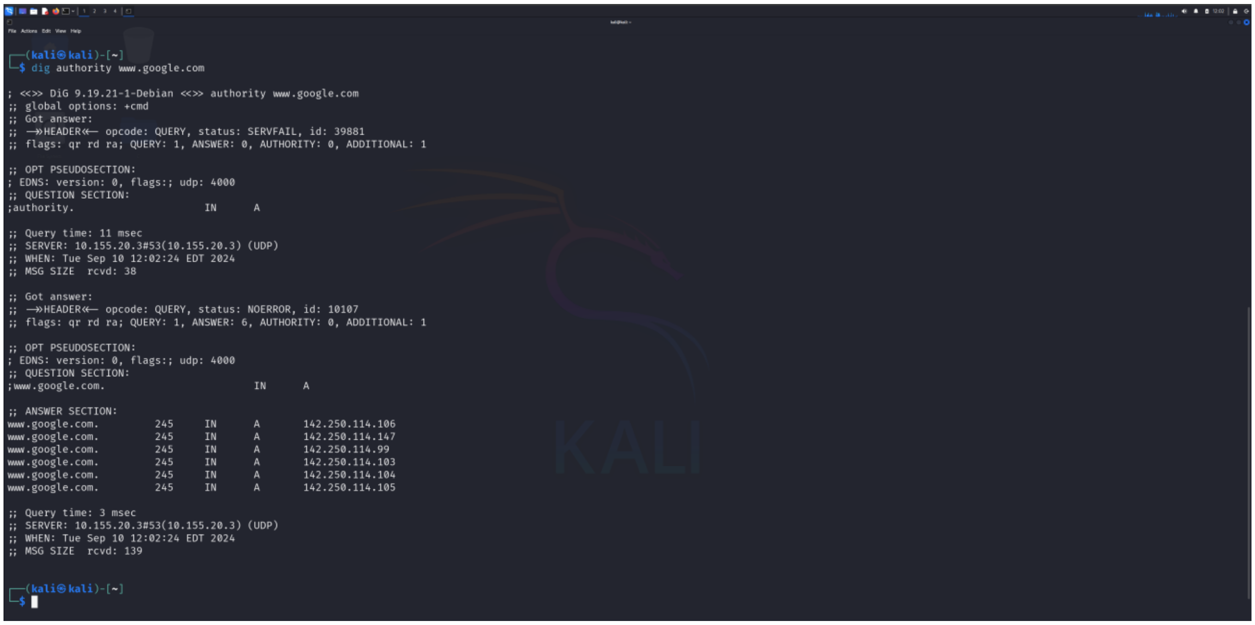
```
┌──(kali㉿kali)-[~]
└─$ dig -h
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
            {global-d-opt} host [@local-server] {local-d-opt}
            [ host [@local-server] {local-d-opt} [ ... ]]
Where:  domain    is in the Domain Name System
        q-class  is one of (in,hs,ch, ... ) [default: in]
        q-type   is one of (a,any,mx,ns,soa,hinfo,axfr,txt, ... ) [default:a]
                 (Use ixfr=version for type ixfr)
        q-opt    is one of:
                 -4                  (use IPv4 query transport only)
                 -6                  (use IPv6 query transport only)
                 -b address[#port]   (bind to source address/port)
                 -c class            (specify query class)
                 -f filename         (batch mode)
                 -k keyfile          (specify tsig key file)
                 -m                  (enable memory usage debugging)
                 -p port             (specify port number)
                 -q name             (specify query name)
                 -r                  (do not read ~/.digrc)
                 -t type             (specify query type)
                 -u                  (display times in usec instead of msec)
                 -x dot-notation     (shortcut for reverse lookups)
                 -y [hmac:]name:key  (specify named base64 tsig key)
        d-opt    is of the form +keyword[=value], where keyword is:
                 +[no]aaflag         (Set AA flag in query (+[no]aaflag))
                 +[no]aaonly         (Set AA flag in query (+[no]aaflag))
                 +[no]additional     (Control display of additional section)
                 +[no]adflag         (Set AD flag in query (default on))
                 +[no]all            (Set or clear all display flags)
                 +[no]answer         (Control display of answer section)
                 +[no]authority      (Control display of authority section)
                 +[no]badcookie      (Retry BADCOOKIE responses)
                 +[no]besteffort     (Try to parse even illegal messages)
                 +bufsize[=###]      (Set EDNS0 Max UDP packet size)
                 +[no]cdflag         (Set checking disabled flag in query)
                 +[no]class          (Control display of class in records)
                 +[no]cmd            (Control display of command line -
                                      global option)
                 +[no]comments       (Control display of packet header
                                      and section name comments)
                 +[no]cookie         (Add a COOKIE option to the request)
                 +[no]crypto         (Control display of cryptographic
                                      fields in records)
                 +[no]defname        (Use search list (+[no]search))
                 +[no]dns64prefix    (Get the DNS64 prefixes from ipv4only.arpa)
                 +[no]dnssec         (Request DNSSEC records)
                 +domain=###         (Set default domainname)
                 +[no]edns[=###]     (Set EDNS version) [0]
                 +ednsflags=###      (Set EDNS flag bits)
                 +[no]ednsnegotiation (Set EDNS version negotiation)
                 +ednsopt=###[:value] (Send specified EDNS option)
                 +noednsopt          (Clear list of +ednsopt options)
                 +[no]expandaaaa     (Expand AAAA records)
                 +[no]expire         (Request time to expire)
                 +[no]fail           (Don't try next server on SERVFAIL)
                 +[no]header-only    (Send query without a question section)
                 +[no]https[=###]    (DNS-over-HTTPS mode) [/]
                 +[no]https-get      (Use GET instead of default POST method while using HTTPS)
                 +[no]http-plain[=###]    (DNS over plain HTTP mode) [/]
                 +[no]http-plain-get      (Use GET instead of default POST method while using plain HTTP)
                 +[no]identify       (ID responders in short answers)
                 +[no]idn            (convert international domain names)
                 +[no]ignore         (Don't revert to TCP for TC responses.)
                 +[no]keepalive      (Request EDNS TCP keepalive)
                 +[no]keepopen       (Keep the TCP socket open between queries)
                 +[no]multiline      (Print records in an expanded format)
                 +ndots=###          (Set search NDOTS value)
```

- I performed dig authority command on Texas A&M University San Antonio's website address.



```
┌──(kali㉿kali)-[~]
└─$ dig authority www.tamusa.edu

; <<>> DiG 9.19.21-1-Debian <<>> authority www.tamusa.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 51703
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;authority.                     IN      A

;; Query time: 19 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 11:59:47 EDT 2024
;; MSG SIZE  rcvd: 38

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25005
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.tamusa.edu.                        IN      A

;; ANSWER SECTION:
www.tamusa.edu.         118     IN      CNAME   satmproxy1idz.tamusa.tamus.edu.
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.132
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.131

;; Query time: 7 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 11:59:47 EDT 2024
;; MSG SIZE  rcvd: 116


┌──(kali㉿kali)-[~]
└─$ ▌
```

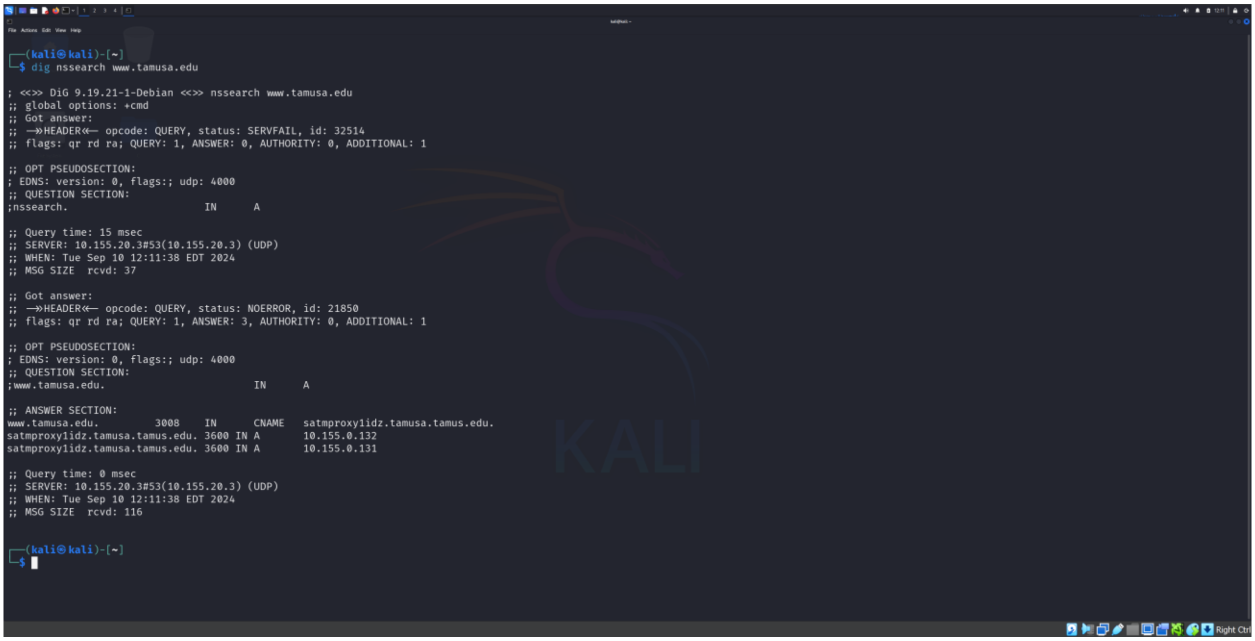
❖ I compared it to using the same command but on Google’s web address.



```
┌──(kali㉿kali)-[~]
└─$ dig authority www.google.com

; <<>> DiG 9.19.21-1-Debian <<>> authority www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 39881
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;authority.                     IN      A

;; Query time: 11 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:02:24 EDT 2024
;; MSG SIZE  rcvd: 38

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10107
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         245     IN      A       142.250.114.106
www.google.com.         245     IN      A       142.250.114.147
www.google.com.         245     IN      A       142.250.114.99
www.google.com.         245     IN      A       142.250.114.103
www.google.com.         245     IN      A       142.250.114.104
www.google.com.         245     IN      A       142.250.114.105

;; Query time: 3 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:02:24 EDT 2024
;; MSG SIZE  rcvd: 139


┌──(kali㉿kali)-[~]
└─$ ▌
```

❖ **I noticed that using the command dig authority on Google’s web address had a faster query time and more Ip addresses in the Answer section. Additionally, the University’s had different web address names answering while Google’s had the same web address answering (though they were different Ip address names).**

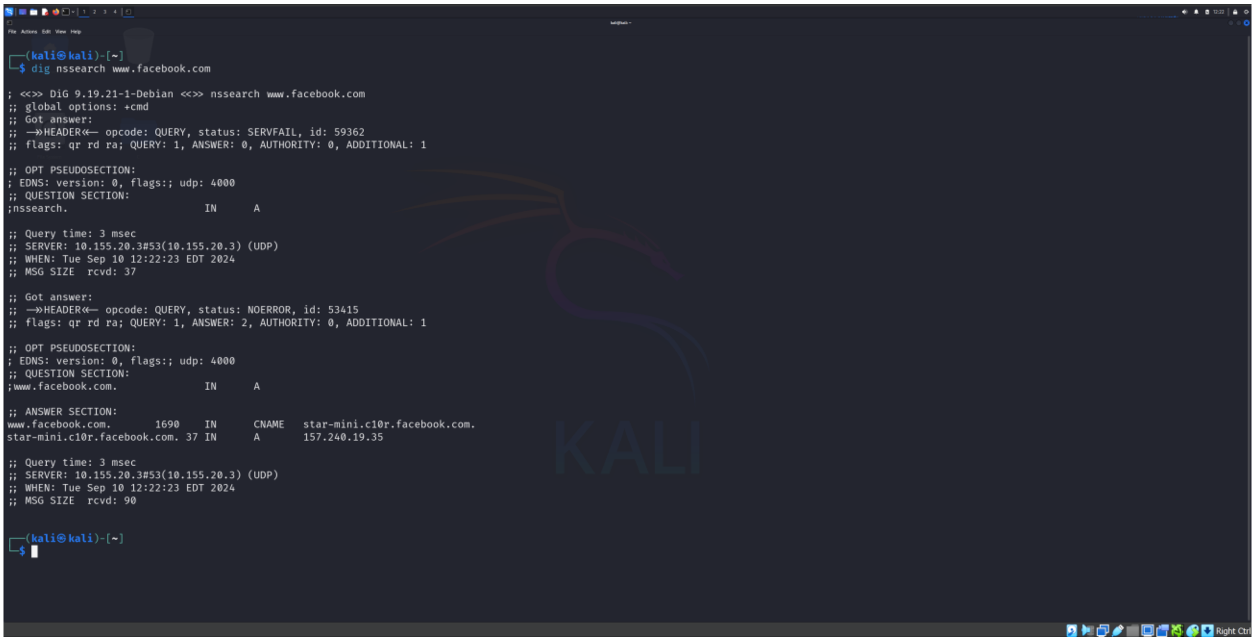
- Then I ran dig nssearch command on Texas A&M University San Antonio’s web address.



```
┌──(kali㉿kali)-[~]
└─$ dig nssearch www.tamusa.edu

; <<>> DiG 9.19.21-1-Debian <<>> nssearch www.tamusa.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32514
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;nssearch.                      IN      A

;; Query time: 15 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:11:38 EDT 2024
;; MSG SIZE  rcvd: 37

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21850
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.tamusa.edu.                        IN      A

;; ANSWER SECTION:
www.tamusa.edu.         3008    IN      CNAME   satmproxy1idz.tamusa.tamus.edu.
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.132
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.131

;; Query time: 0 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:11:38 EDT 2024
;; MSG SIZE  rcvd: 116


┌──(kali㉿kali)-[~]
└─$ 
```

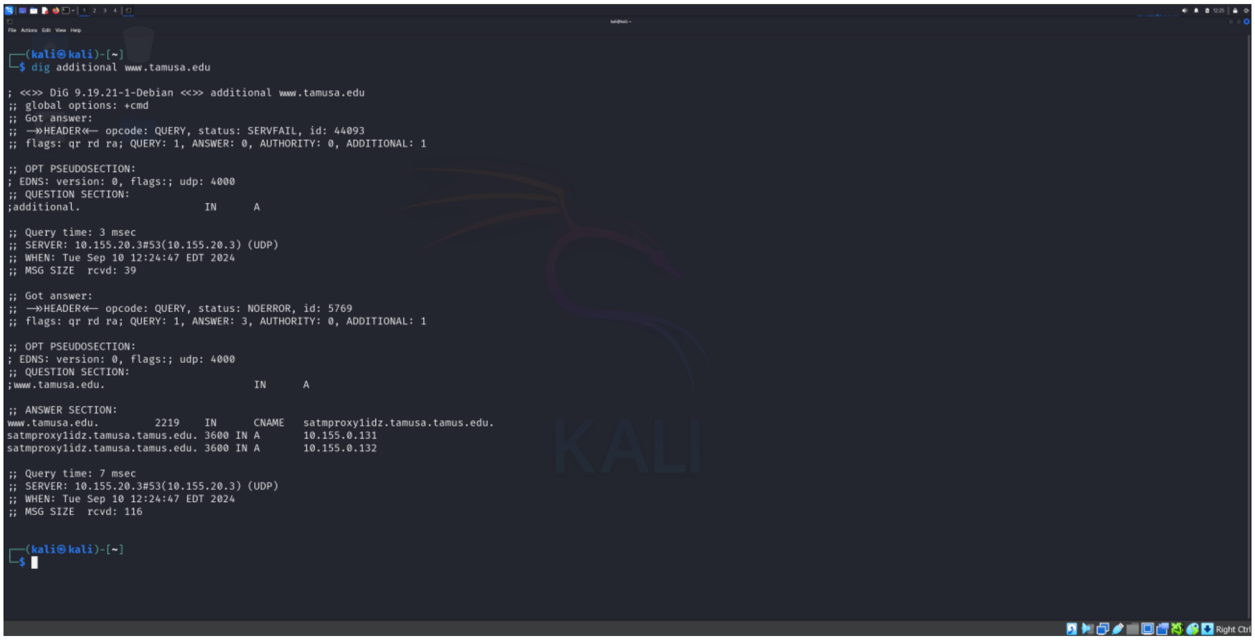
- **Dig nssearch command on Texas A&M University San Antonio’s web address populated with faster query time then dig authority command. Additionally, the Ip address for satmproxylidz.tamus.edu both were different then when I ran dig authority command.**

- Then I tried same command on Facebook

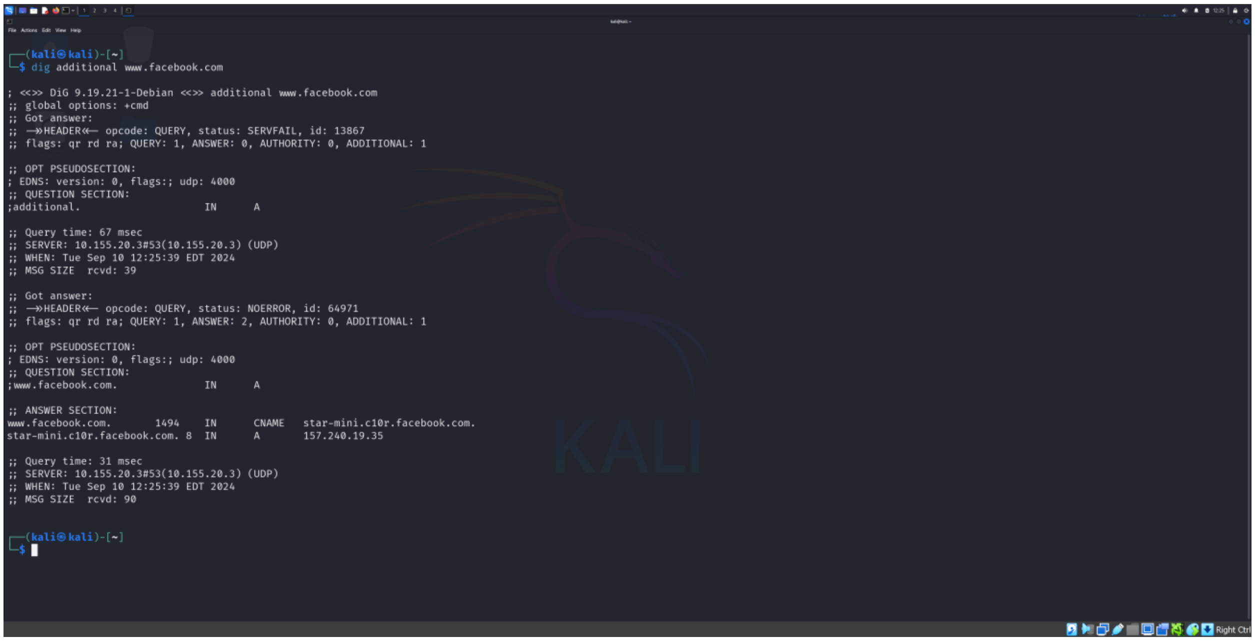


```
┌──(kali㉿kali)-[~]
└─$ dig nssearch www.facebook.com

; <<>> DiG 9.19.21-1-Debian <<>> nssearch www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 59362
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;nssearch.                      IN      A

;; Query time: 3 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:22:23 EDT 2024
;; MSG SIZE  rcvd: 37

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53415
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       1690    IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 37 IN      A       157.240.19.35

;; Query time: 3 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:22:23 EDT 2024
;; MSG SIZE  rcvd: 90


┌──(kali㉿kali)-[~]
└─$ 
```

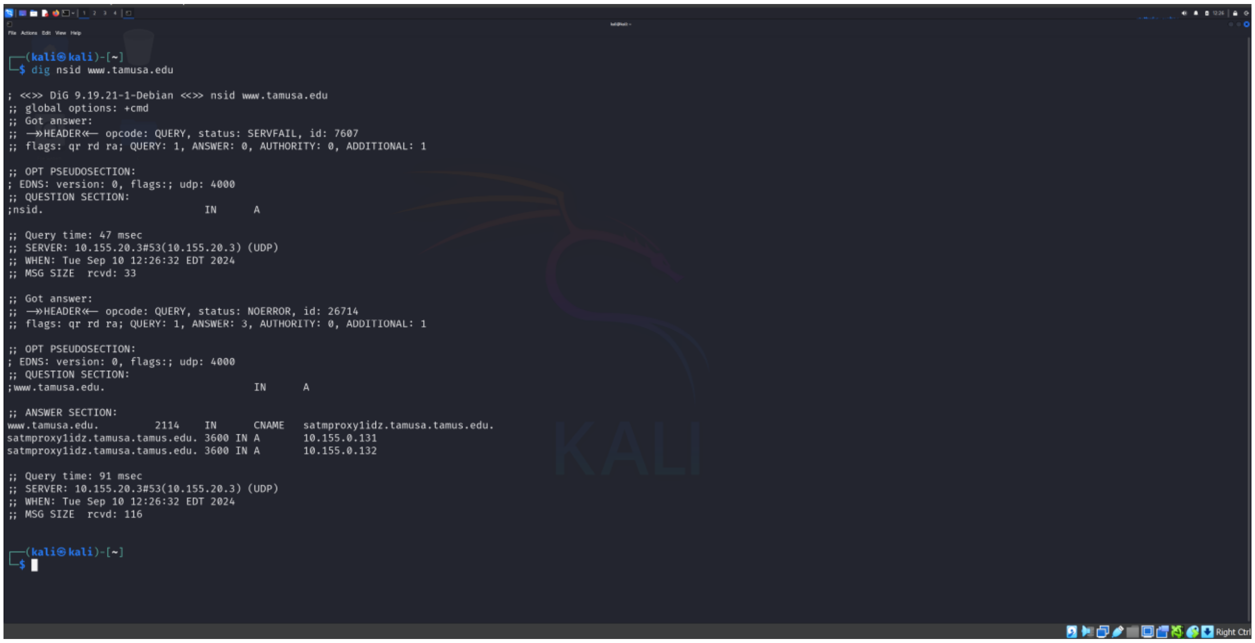
- Finally, I ran additional dig commands on Texas A&M University San Antonio and Fakebooks' web address.



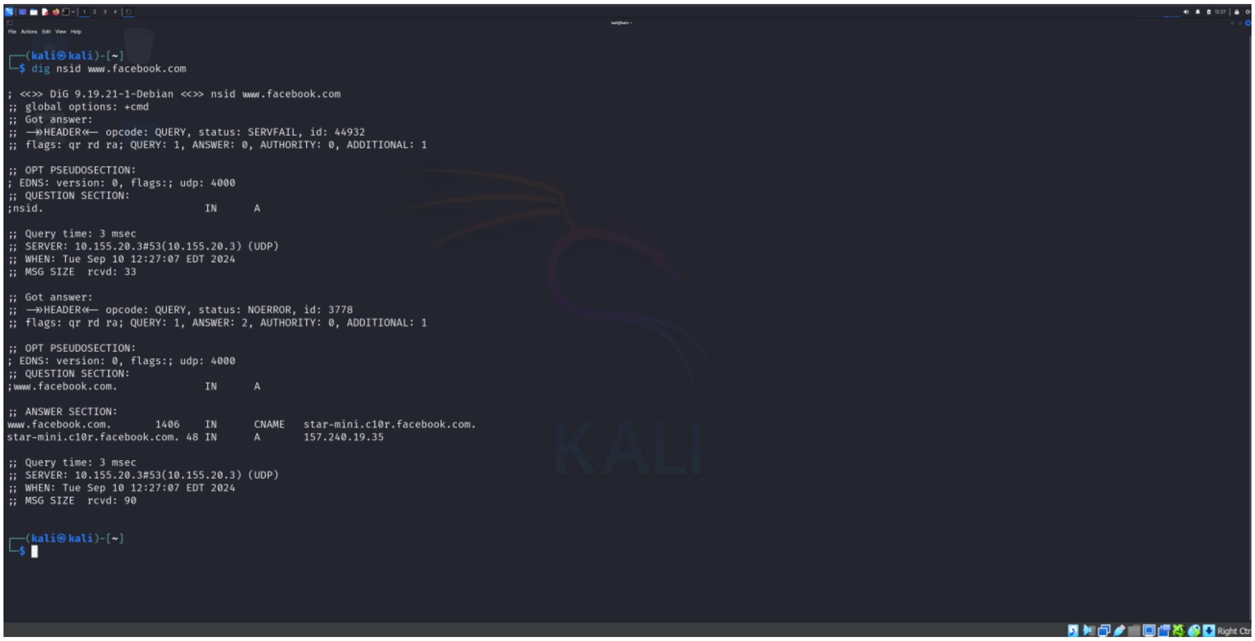
```
┌──(kali㉿kali)-[~]
└─$ dig additional www.tamusa.edu

; <<>> DiG 9.19.21-1-Debian <<>> additional www.tamusa.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 44093
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;additional.                    IN      A

;; Query time: 3 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:24:47 EDT 2024
;; MSG SIZE  rcvd: 39

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5769
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.tamusa.edu.                        IN      A

;; ANSWER SECTION:
www.tamusa.edu.         2219    IN      CNAME   satmproxy1idz.tamusa.tamus.edu.
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.131
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.132

;; Query time: 7 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:24:47 EDT 2024
;; MSG SIZE  rcvd: 116


┌──(kali㉿kali)-[~]
└─$ 
```



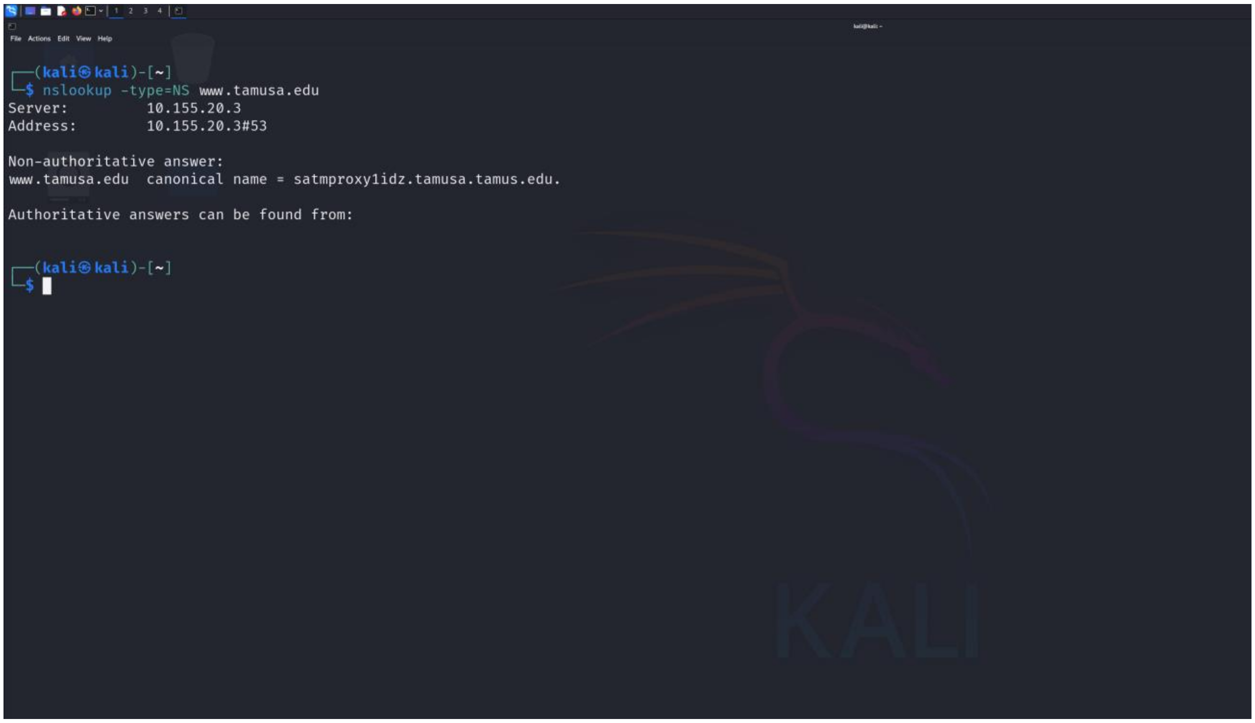
```
┌──(kali㉿kali)-[~]
└─$ dig additional www.facebook.com

; <<>> DiG 9.19.21-1-Debian <<>> additional www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 13867
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;additional.                    IN      A

;; Query time: 67 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:25:39 EDT 2024
;; MSG SIZE  rcvd: 39

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64971
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       1494    IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 8  IN      A       157.240.19.35

;; Query time: 31 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:25:39 EDT 2024
;; MSG SIZE  rcvd: 90


┌──(kali㉿kali)-[~]
└─$ 
```



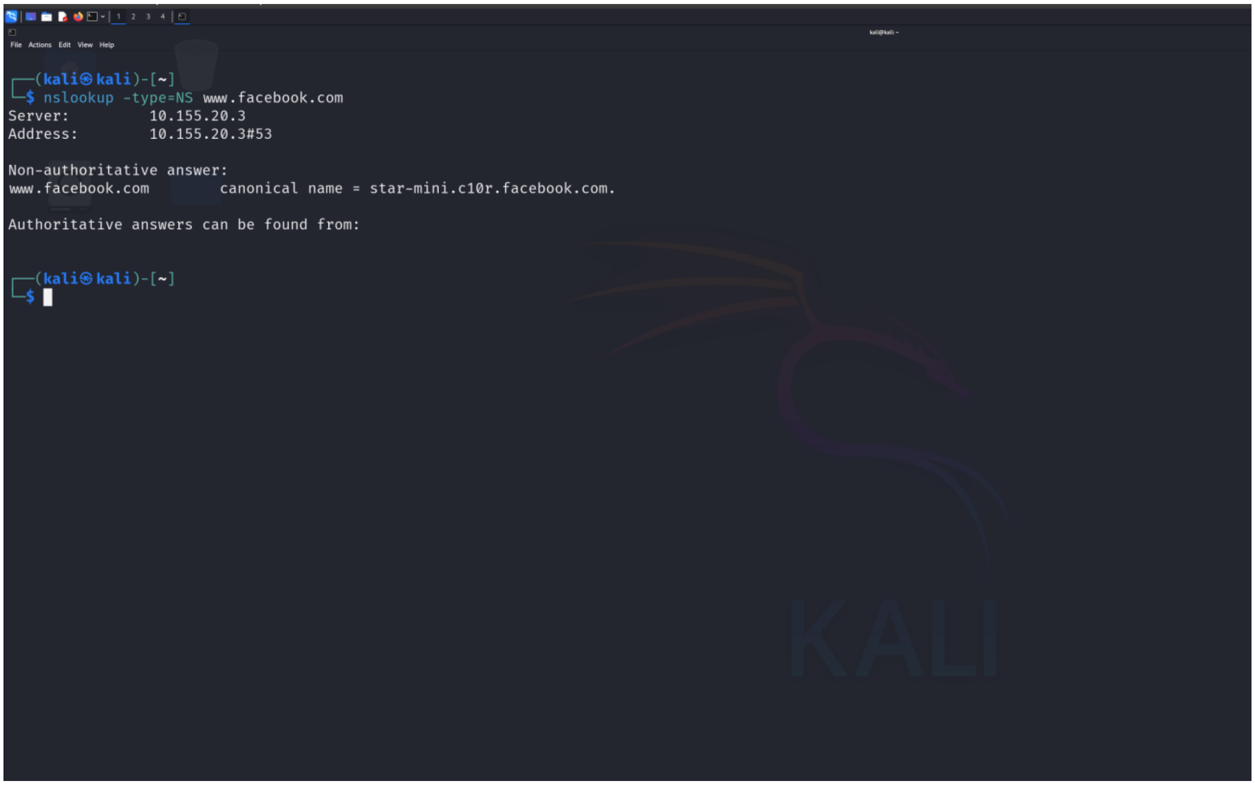
```
┌──(kali㉿kali)-[~]
└─$ dig nsid www.tamusa.edu

; <<>> DiG 9.19.21-1-Debian <<>> nsid www.tamusa.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 7607
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;nsid.                          IN      A

;; Query time: 47 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:26:32 EDT 2024
;; MSG SIZE  rcvd: 33

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26714
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.tamusa.edu.                        IN      A

;; ANSWER SECTION:
www.tamusa.edu.         2114    IN      CNAME   satmproxy1idz.tamusa.tamus.edu.
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.131
satmproxy1idz.tamusa.tamus.edu. 3600 IN A       10.155.0.132

;; Query time: 91 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:26:32 EDT 2024
;; MSG SIZE  rcvd: 116


┌──(kali㉿kali)-[~]
└─$ 
```



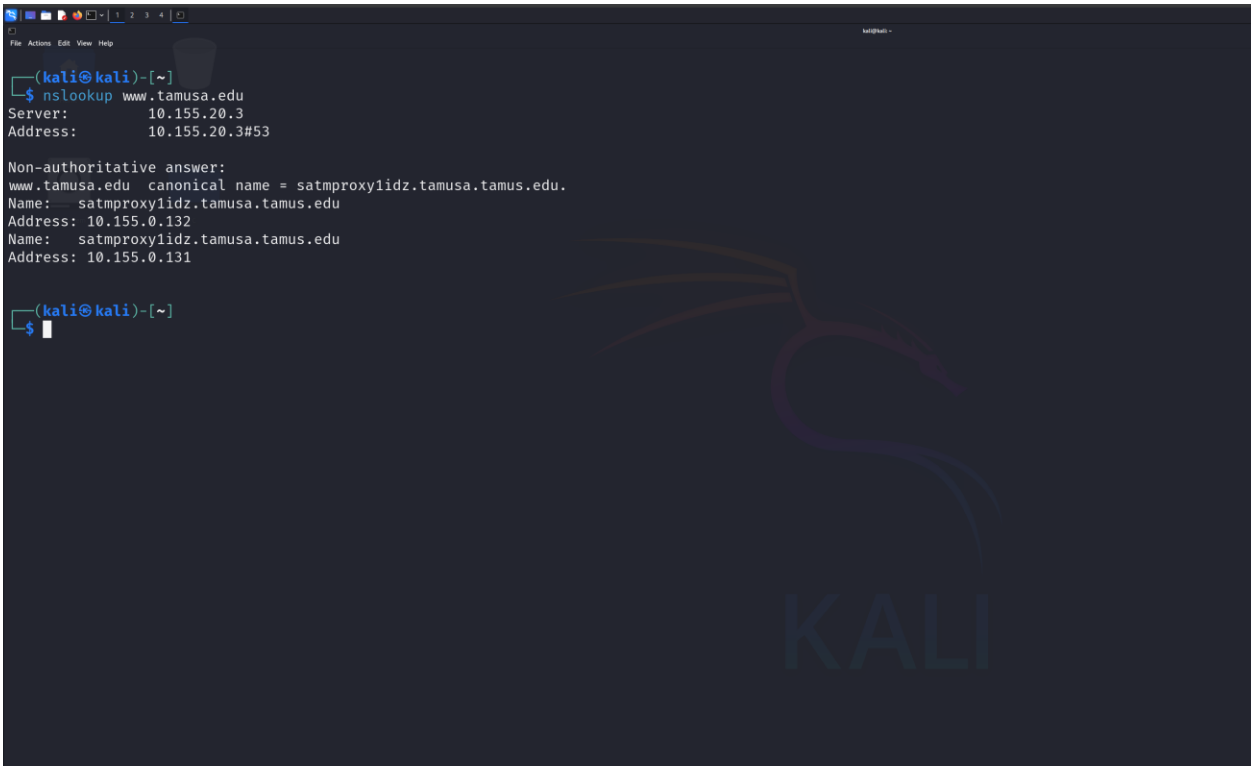
```
┌──(kali㉿kali)-[~]
└─$ dig nsid www.facebook.com

; <<>> DiG 9.19.21-1-Debian <<>> nsid www.facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 44932
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;nsid.                          IN      A

;; Query time: 3 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:27:07 EDT 2024
;; MSG SIZE  rcvd: 33

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3778
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       1406    IN      CNAME   star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com. 48 IN      A       157.240.19.35

;; Query time: 3 msec
;; SERVER: 10.155.20.3#53(10.155.20.3) (UDP)
;; WHEN: Tue Sep 10 12:27:07 EDT 2024
;; MSG SIZE  rcvd: 90


┌──(kali㉿kali)-[~]
└─$ 
```



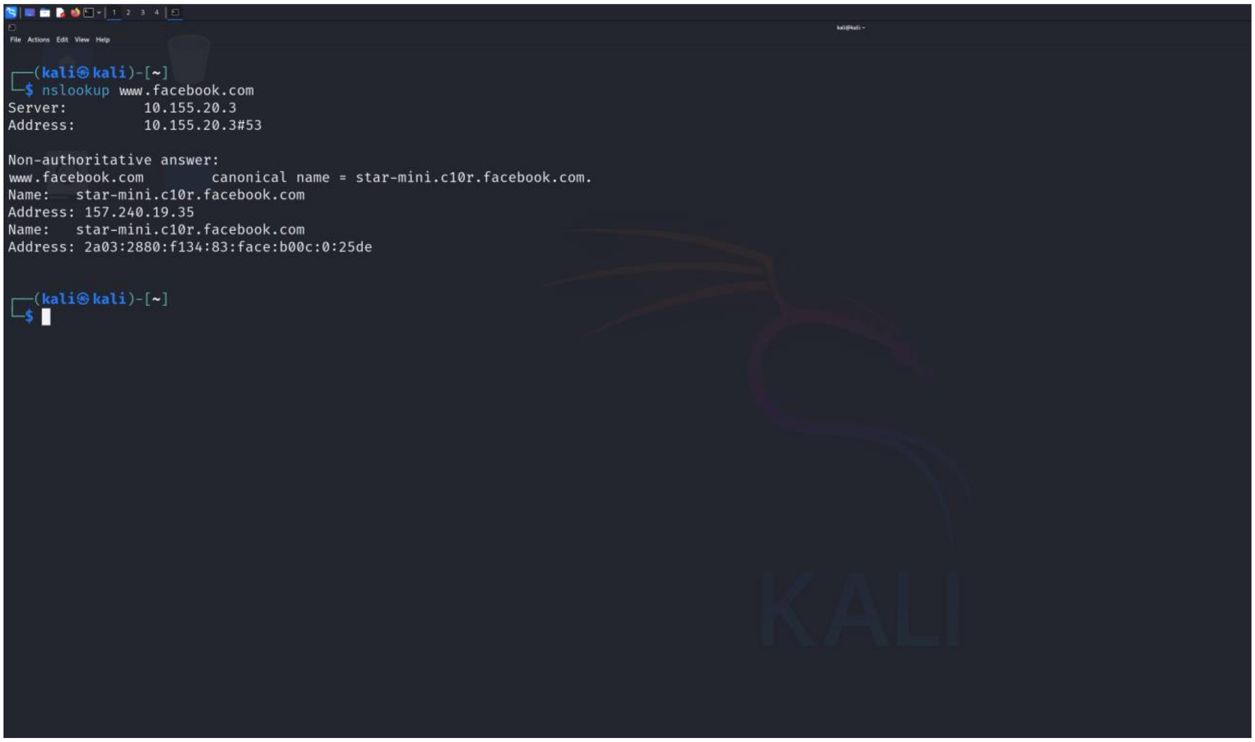
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=NS www.tamusa.edu
Server:         10.155.20.3
Address:        10.155.20.3#53

Non-authoritative answer:
www.tamusa.edu  canonical name = satmproxy1idz.tamusa.tamus.edu.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=NS www.facebook.com
Server:         10.155.20.3
Address:        10.155.20.3#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup www.tamusa.edu
Server:         10.155.20.3
Address:        10.155.20.3#53

Non-authoritative answer:
www.tamusa.edu  canonical name = satmproxy1idz.tamusa.tamus.edu.
Name:   satmproxy1idz.tamusa.tamus.edu
Address: 10.155.0.132
Name:   satmproxy1idz.tamusa.tamus.edu
Address: 10.155.0.131


┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup www.facebook.com
Server:         10.155.20.3
Address:        10.155.20.3#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.19.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f134:83:face:b00c:0:25de


┌──(kali㉿kali)-[~]
└─$ 
```

What I learned:

DNS (Domain Name System) is a fundamental component of the internet that converts human-readable domain names to IP addresses. The dig and Nslookup commands are crucial tools for searching DNS servers. Nslookup is widely available on most Linux operating systems and easy to use for simple DNS queries like checking IP addresses and doing reverse lookups. The dig command (Domain Information Groper) is a more robust and adaptable tool that provides detailed information and supports complex DNS queries, making it the ideal option for system administrators. Both tools are extremely useful for diagnosing and resolving DNS issues.