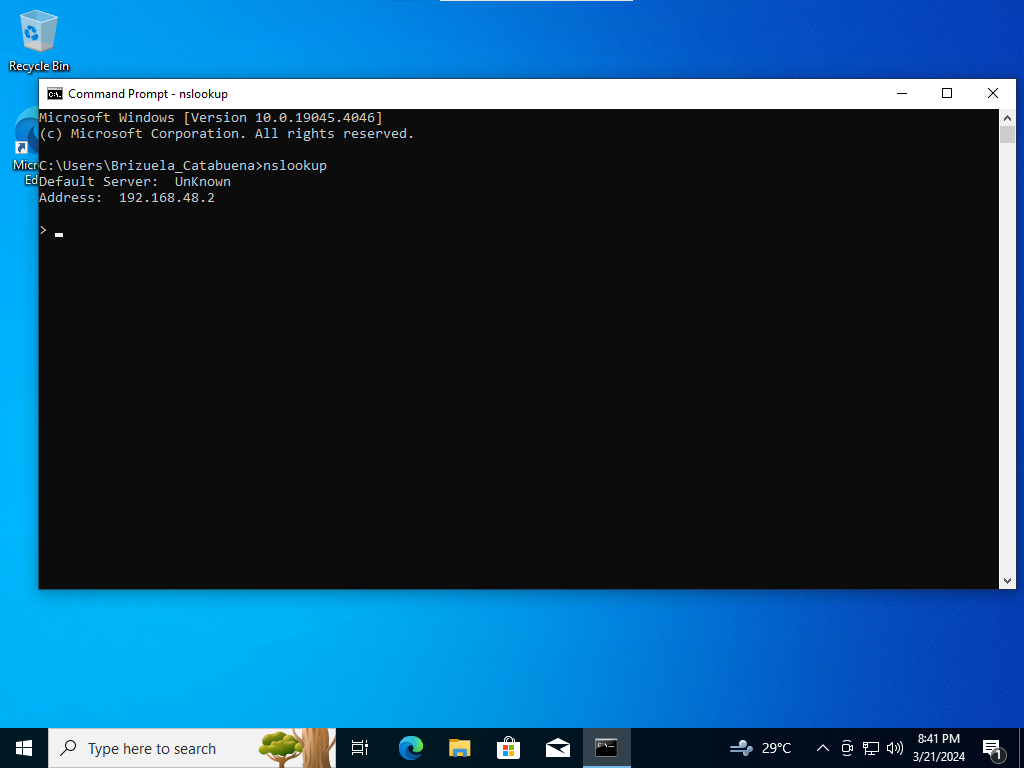
**LAB #2: FOOTPRINTING**

**IT 322 – INFORMATION ASSURANCE AND SECURITY I**

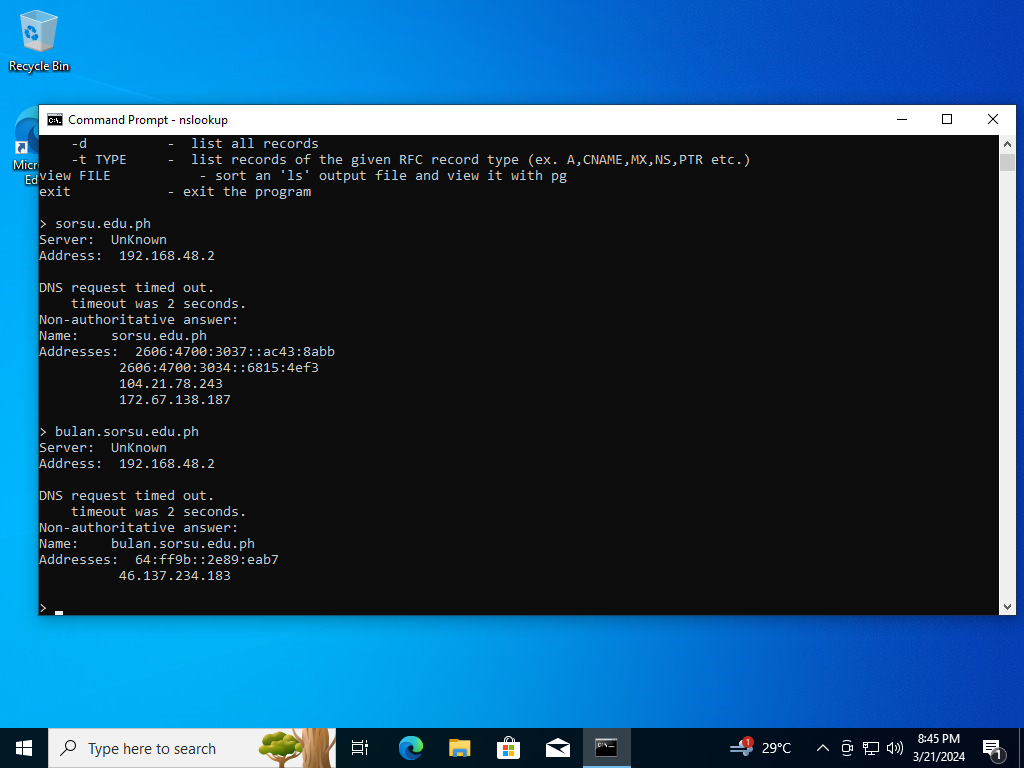
2nd Semester A.Y. 2023-2024

|  |  |
| --- | --- |
| Name: DAZEL M. CATABUENA | Program, Block: **BSIT 3-2** |
| Name of Partner: LEONY B. BRIZUELA | Date: **March 25, 2024** |



NSlookup Default DNS Server

|  |  |
| --- | --- |
| COMMAND | INFORMATION |
| All | Print options, current server and host |
| [no] debug | print debugging information |
| [no] d2 | print exhaustive debugging information |
| [no]defname | append domain name to each query |
| [no]recurse | ask for recursive answer to query |
| [no]search | use domain search list |
| [no]vc | always use a virtual circuit |
| domain=NAME | set default domain name to NAME |
| srchlist=N1[/N2/.../N6] | set domain to N1 and search list to N1,N2, etc. |
| root=NAME | set root server to NAME |
| retry=X | set number of retries to X |
| timeout=X | set initial time-out interval to X seconds |
| type=X | set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV) |
| querytype=X | same as type |
| class=X | set query class (ex. IN (Internet), ANY) |
| [no]msxfr | use MS fast zone transfer |
| ixfrver=X | current version to use in IXFR transfer request |
| server NAME | set default server to NAME, using current default server |
| lserver NAME | set default server to NAME, using initial server |
| root | set current default server to the root |
| ls [opt] DOMAIN [> FILE] | list addresses in DOMAIN (optional: output to FILE) |
| -a | list canonical names and aliases |
| -d | list all records |
| -t TYPE | list records of the given RFC record type (ex. A,CNAME,MX,NS,PTR etc.) |
| view FILE | sort an 'ls' output file and view it with pg |
| exit | exit the program |



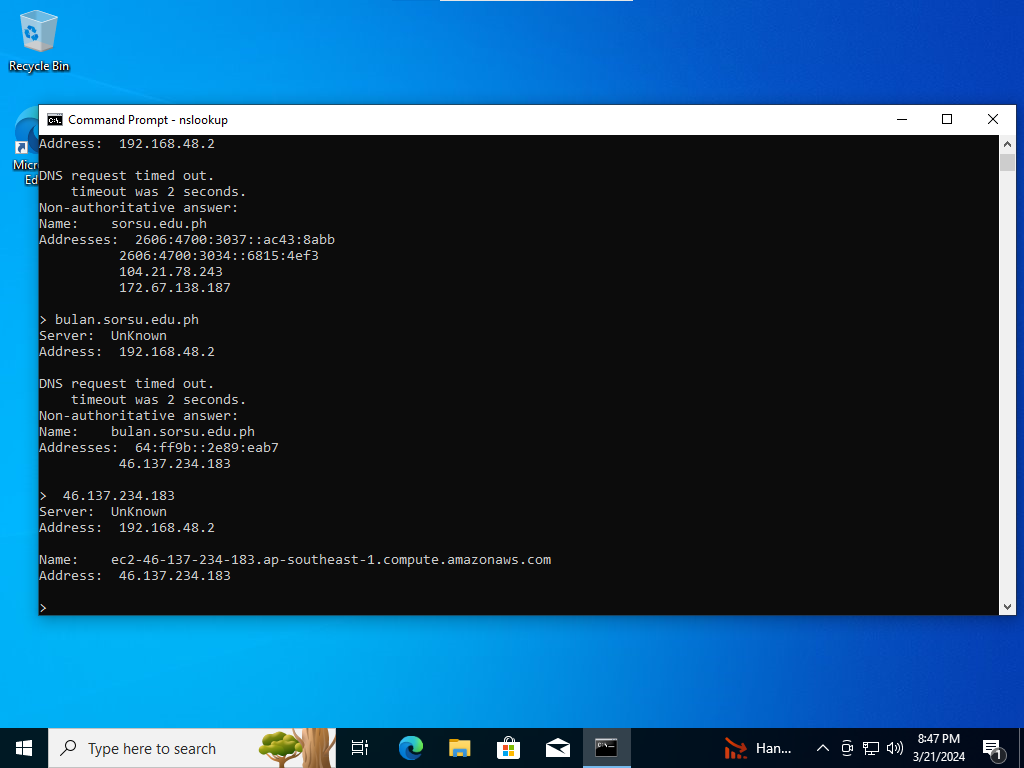
NSlookup IP Lookup

1. Domain Name – sorsu.edu.ph

IP Address – 192.168.48.2

1. Domain Name – bulan.sorsu.edu.ph

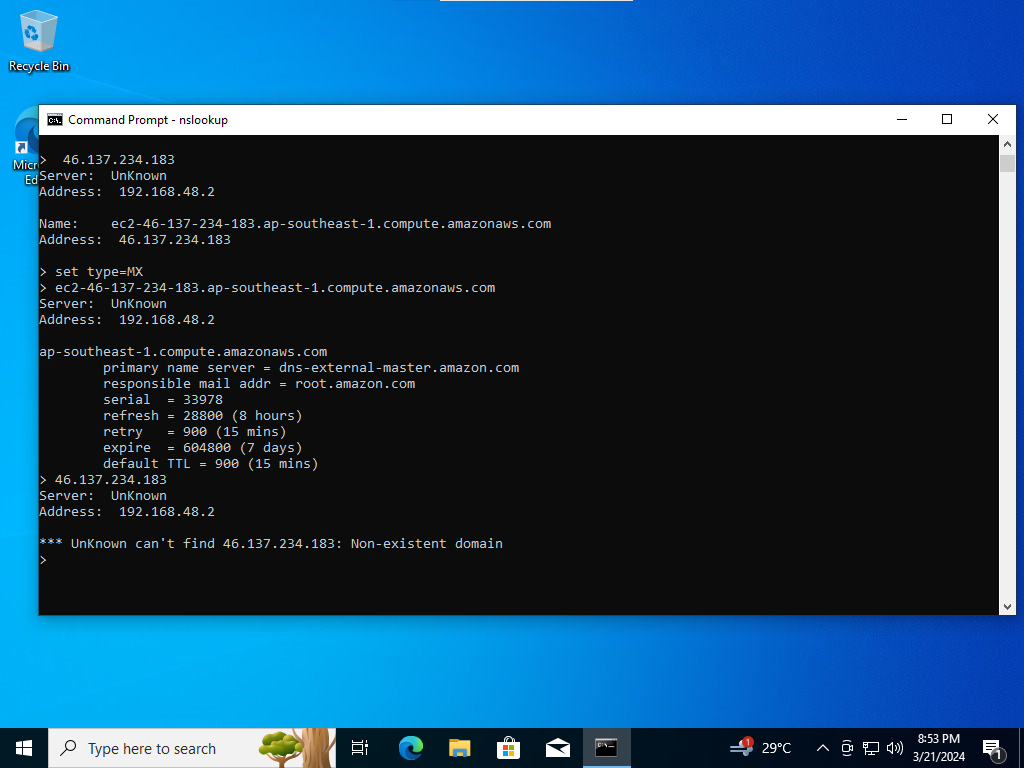
IP Address – 192.168.48.2



NSlookup DNS Reverse Lookup

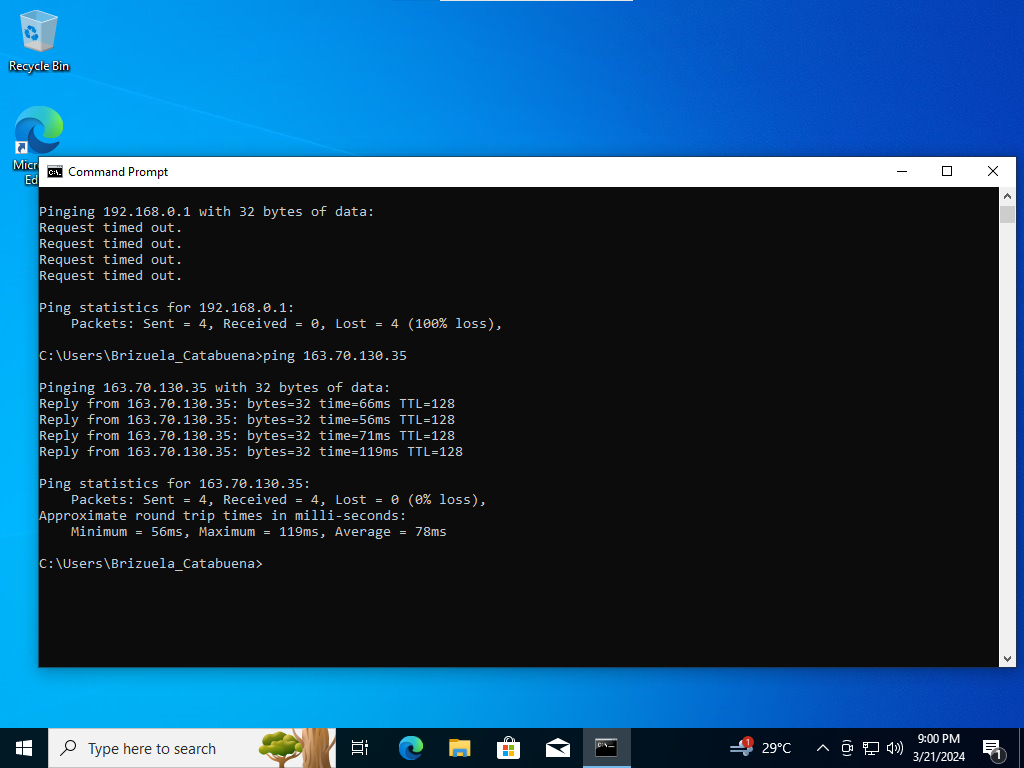
IP Address – 46.137.234.183

Domain Name – ec2-46-137-234-183.ap-southeast-1.computer.amazonaws.com



NSlookup Mail Servers

Primary Name Server – dns-external-master.amazon.com

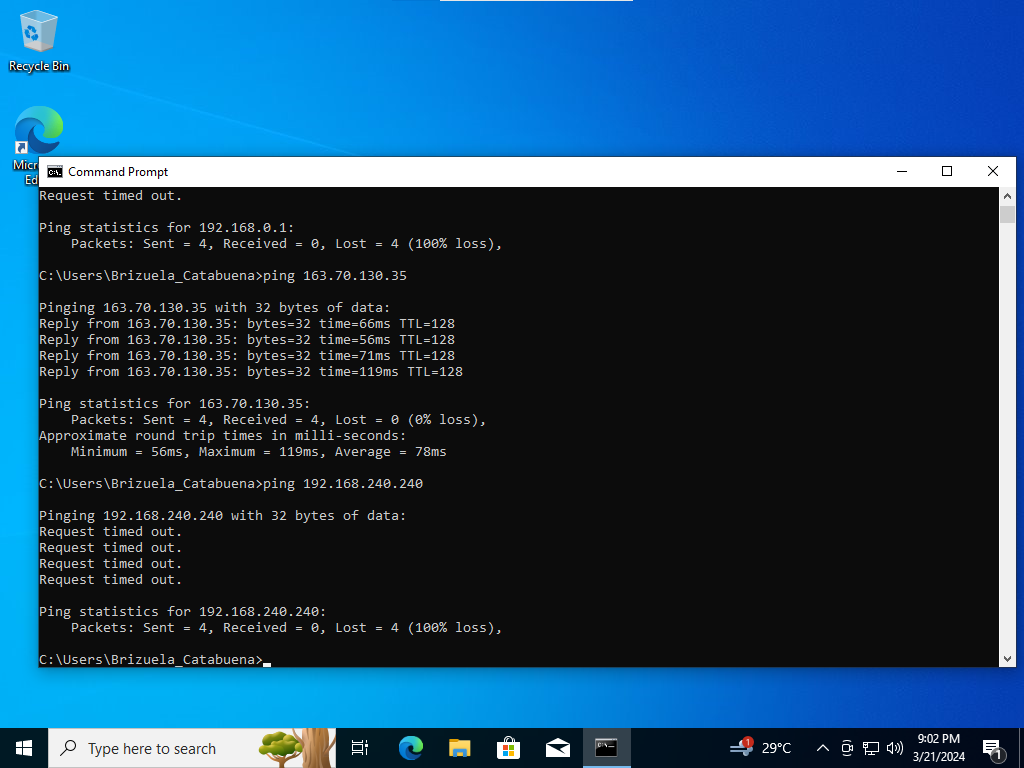


Ping

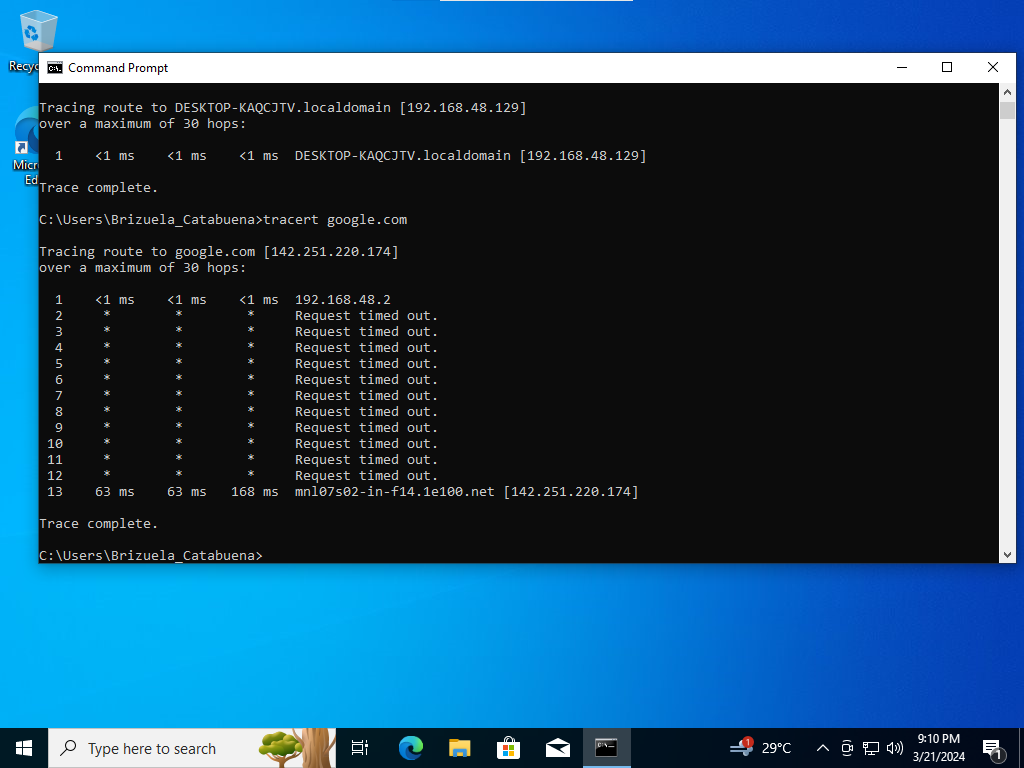
Minimum – 56ms

Maximum – 119ms

Average – 78ms

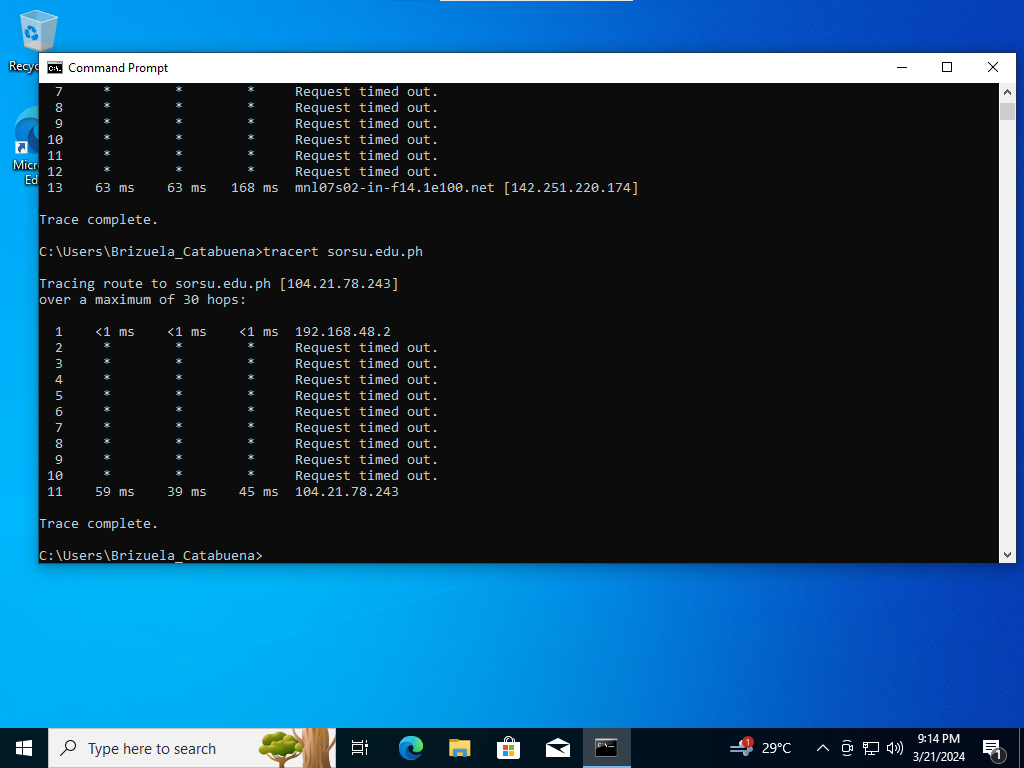


Ping Unreachable Host



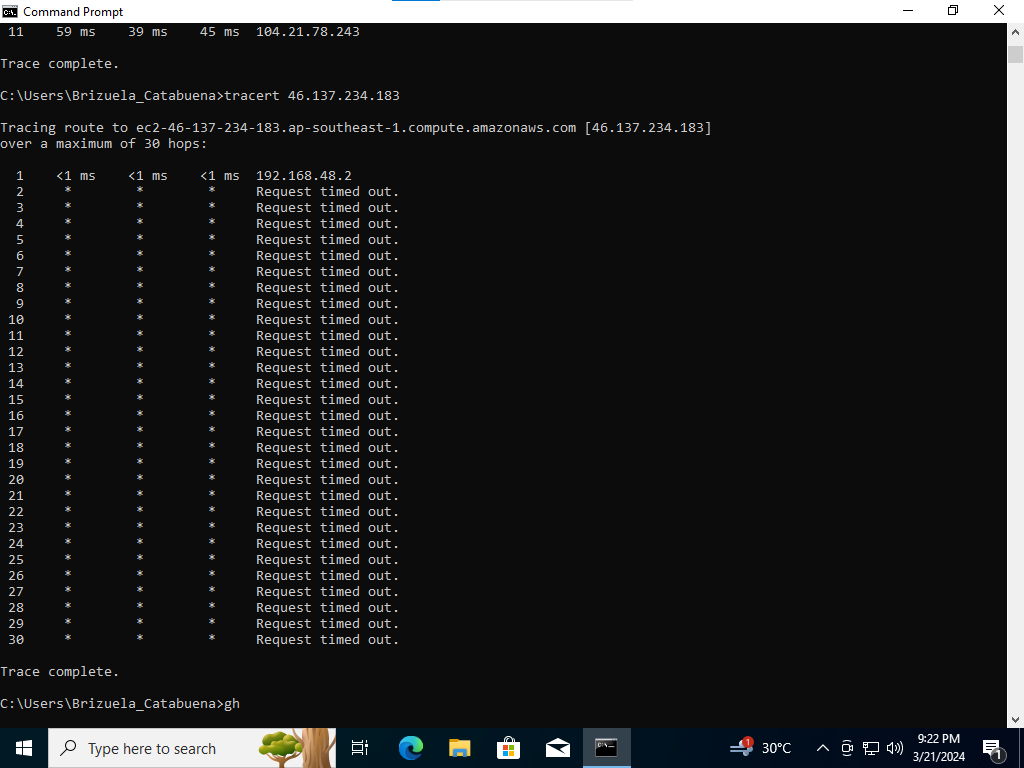
Traceroute with DNS Lookup

Level of Information – 13



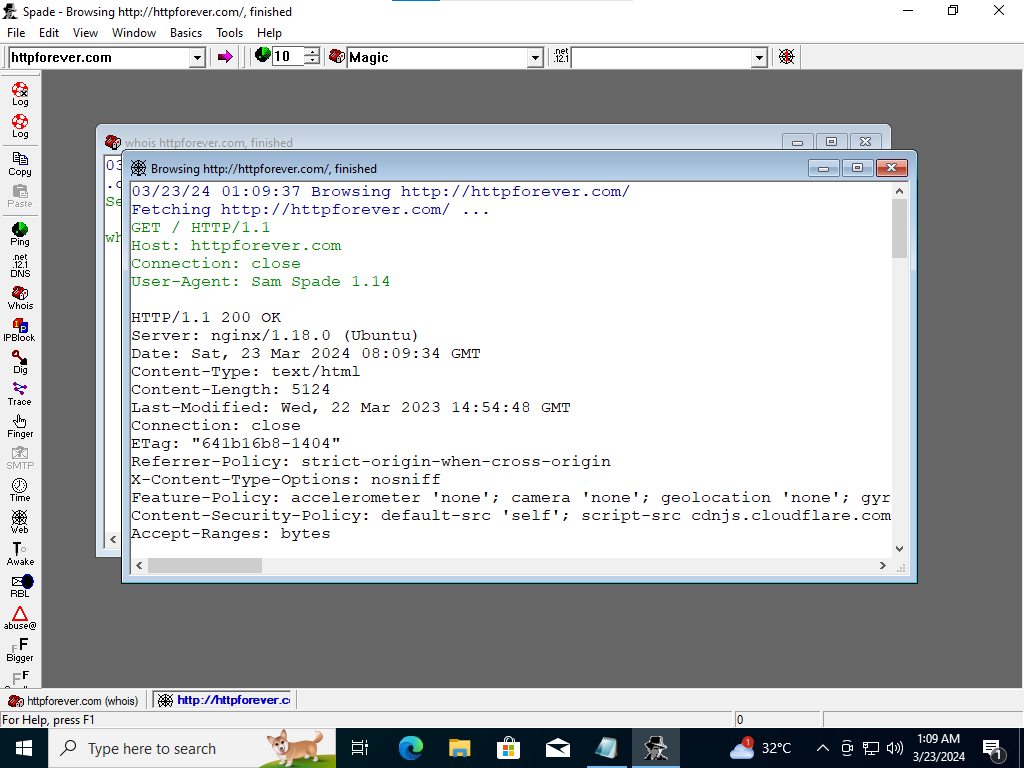
Traceroute with DNS Lookup

Level of Information – 11



Traceroute with DNS Lookup

Level of Information – 30



Web Reconnaissance Using Sam Spade

Who wrote the code?

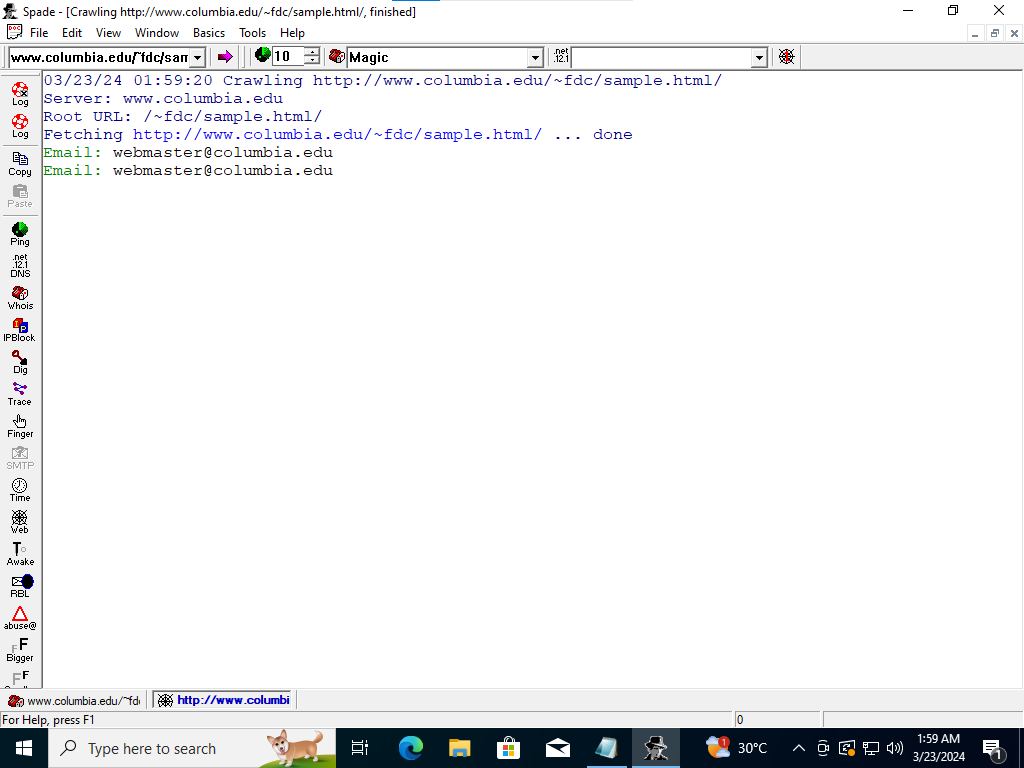
Scott Helme

Web sites located outside the target organization –

Twitter.com and Facebook.com

Link to other web servers located inside the target organization –

<http://httpforever.com/https://www.facebook.com.scott.helme> and [https://www.facebook.com/scott.helme HTTP/1.1](https://www.facebook.com/scott.helme%20HTTP/1.1)

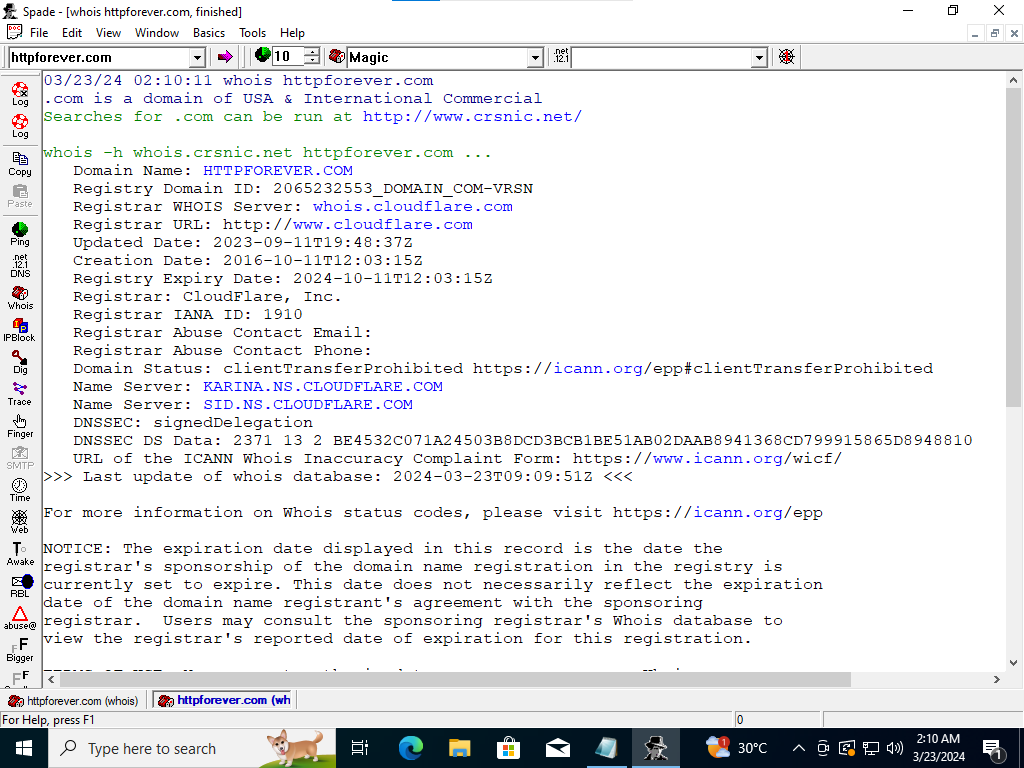


Sam Spade Web Crawling

E-mail Address – [webmaster@columbia.edu](mailto:webmaster@columbia.edu)

Link to other web servers located inside the target organization –

[https://www.columbia.edu/~fdc/sample.html/](https://www.columbia.edu/~fdc/sample.html/?fbclid=IwAR2B1hJzgaE4FeABrFAOKGmcTed1vAV6c43PPIRb0Tr6Yd9lVlNsRzlQnhs) and [http://www.columbia.edu/~fdc/sample.html/](http://www.columbia.edu/~fdc/sample.html/?fbclid=IwAR1llGwRq_s_sRteIVJ0c4cSzYglYzO-RlBf24qLw2CV3p6UvJ5cSY0dth0) ... done



Gathering Whois Information with Sam Spade

Domain Name: HTTP FOREVER.COM Registry

Domain ID: 2065232553\_DOMAIN\_COM-VRSN

Registry WHOIS Server: whois.cloudflare.com

Registrar URL: [https://www.cloudflare.com](https://www.cloudflare.com/?fbclid=IwAR1G-ytvi7dglm3TmgV9JQ77xgaGm2C4M2dXG_UKkE3azwpqVKqgD5qlraw)

Update Date: 2023-09-11T19:48:37z

Creation Date: 2016-10-11T12:03:15z

Registry Expiry Date: 2024-10-11T12:03:15z

Registrar: CloudFlare, Inc. Registrar IANA ID: 1910

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone:

Domain Status: clientTransferProhibited [https://ICANN.org/epp#clientTransferProhibited](https://icann.org/epp?fbclid=IwAR3ZUv40RvYaLQIJc9oNBZKxwB0kQ8yygZsNETMcx3qXwE3W3BW9QaNX_bQ#clientTransferProhibited)

Name Server: KARINA.NS.CLOUDFLARE.COM

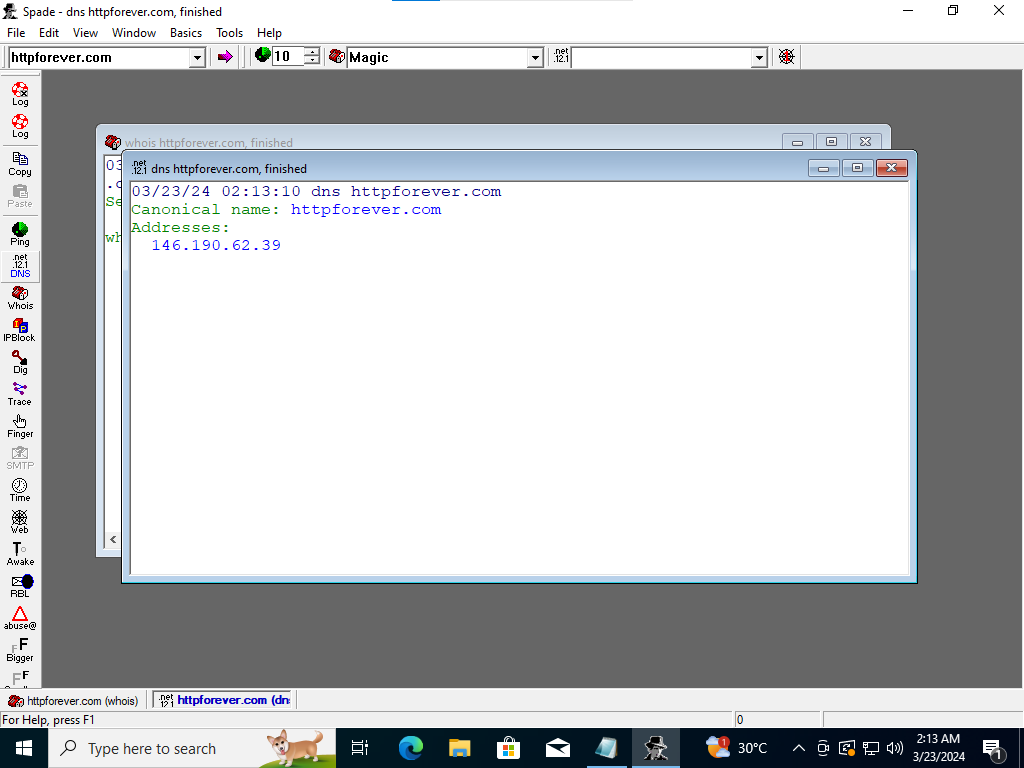
Name Server: SID.NS.CLOUDFLARE.COM

DNSSEC: signed delegation

DNSSEC DS Data: 2317 13 2 BE4532C071A24503B8DCD3BCB1BE51AB02DAAB8941368CD799915865D8948810

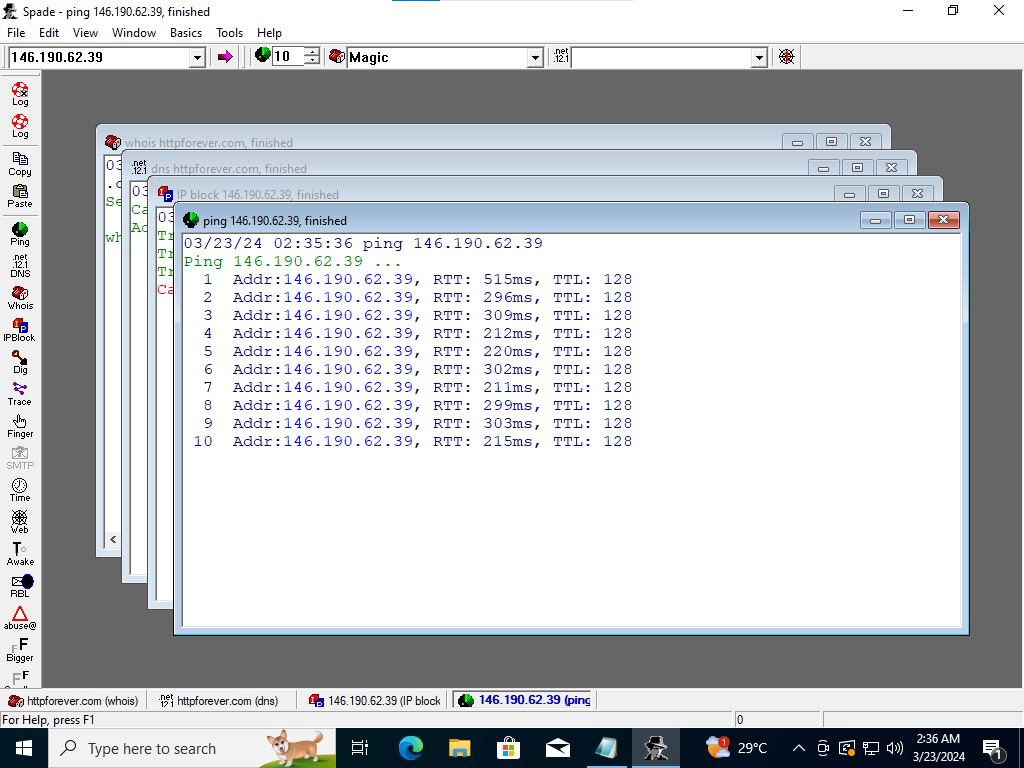
URL of the ICANN Whois Inaccuracy Complaint Form: [https://www.icann.org/wicf/](https://www.icann.org/wicf/?fbclid=IwAR0sFCv2wPEoyA1P-b3wnc1DEuOd_ubdZkAkVjIXEPENci9dkC8fRTAqj-s)

Last Update of Whois Database: 2024-03-23T09:09:51z



Sam Spade DNS Query

DNS Address – 146.190.62.39

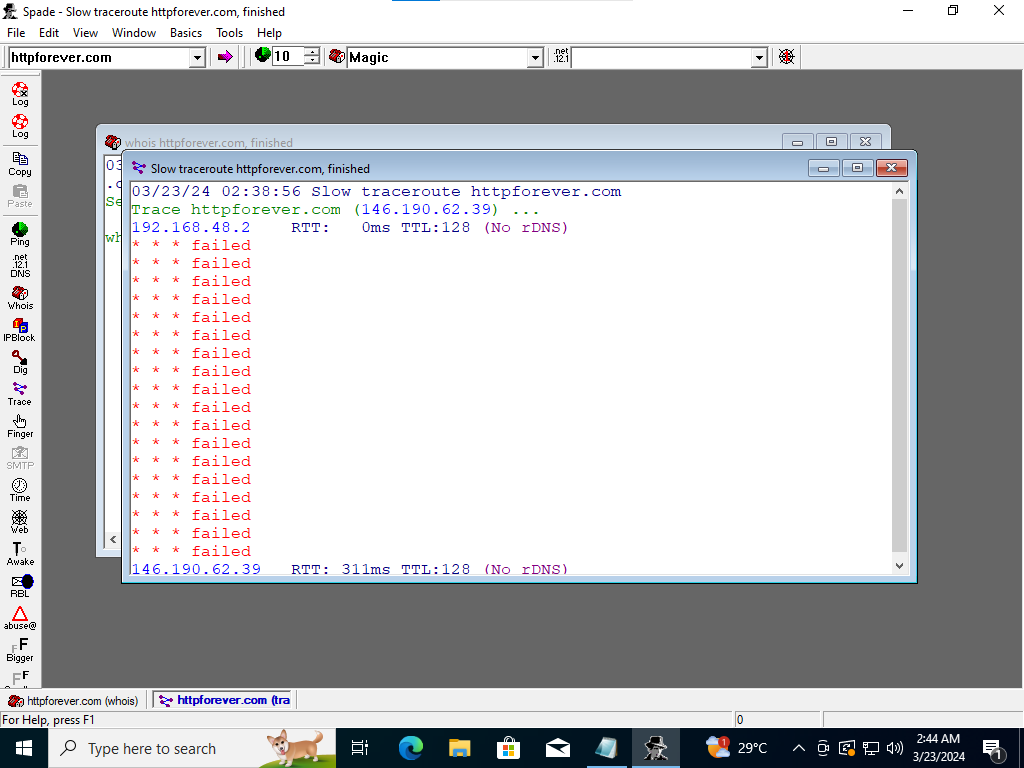


Sam Spade Ping

Minimum – 211ms

Maximum – 515ms

Average – 296ms



Sam Spade Traceroute

Output of the Traceroute – Failed