LAB01 Foot Printing

Class: M03 Student ID: B2111933 Name: Truong Dang Truc Lam

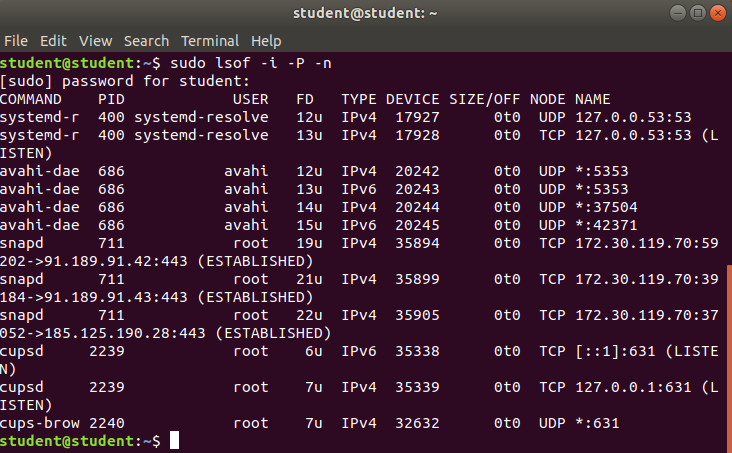
| Model | Area | Tools | Remark |
| --- | --- | --- | --- |
| [model A] | server and the services  detection | Lsof command | OS command |
| banner grabbing | Whatweb | tool |
| OS detection | netcraft. | tool |
| [model B] | dig (domain information groper) | dig command | DNS (Domain Name System) |
| [model C] | tool | Samspade | site |

**Select one model**

**[model A]**

1. Display the list of all open files in a server and the services that have opened them and explain the test result.

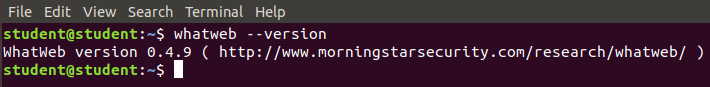
# sudo lsof -i -P –n



This server is actively handling DNS resolution, Snap package management, zeroconf networking, and printing services. It has both local and external network connections established. Most services are bound to specific addresses or ports relevant to their function.

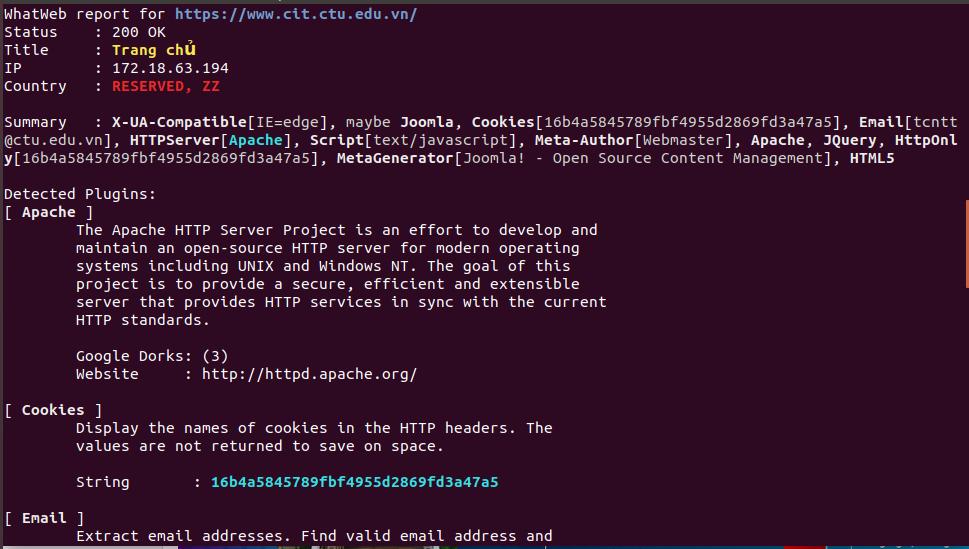
1. Execute Whatweb banner grabbing using Kali Linux or Ubuntu and explain the test result.

<https://linux-packages.com/ubuntu-focal-fossa/package/whatweb>



Installed Whatweb

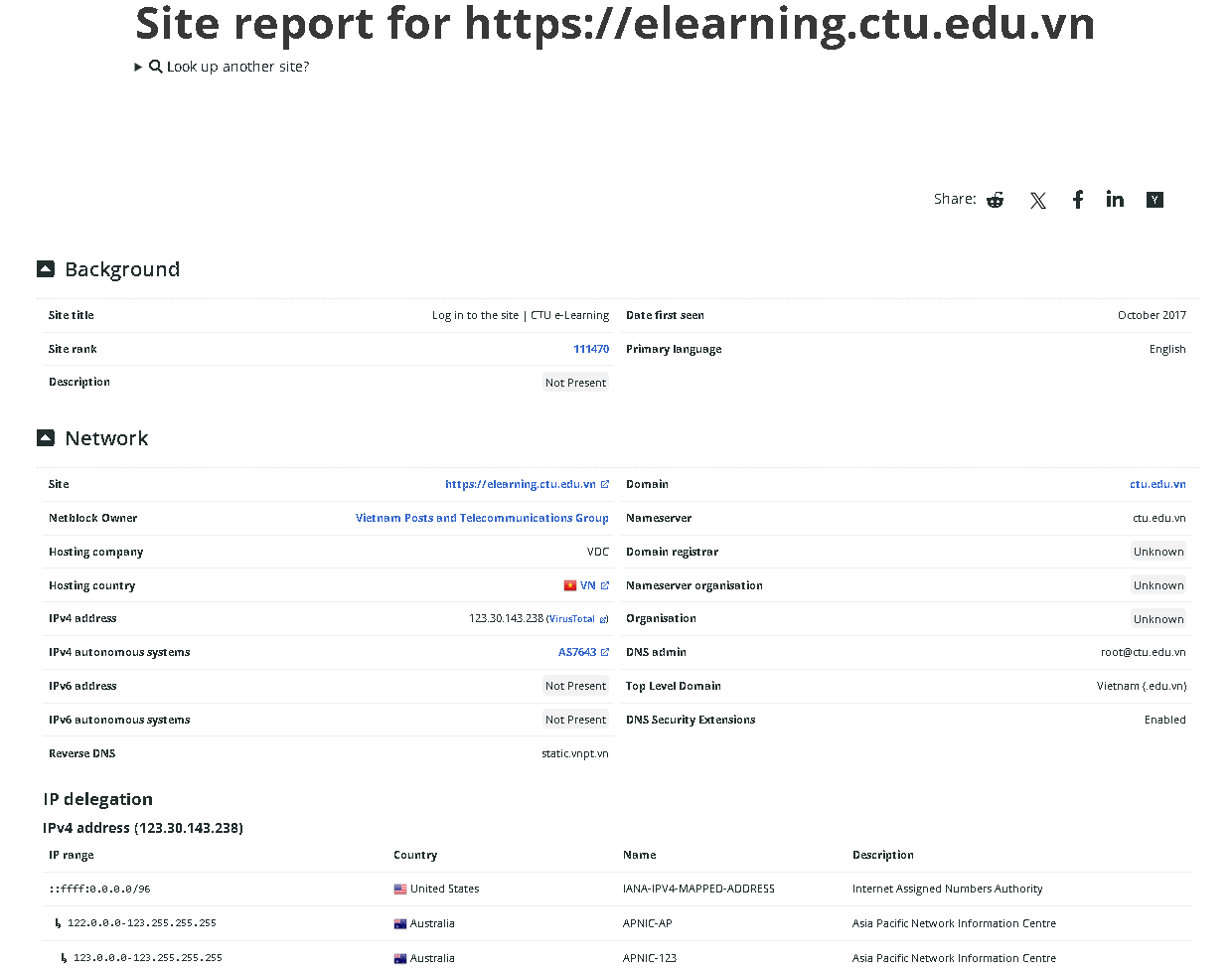




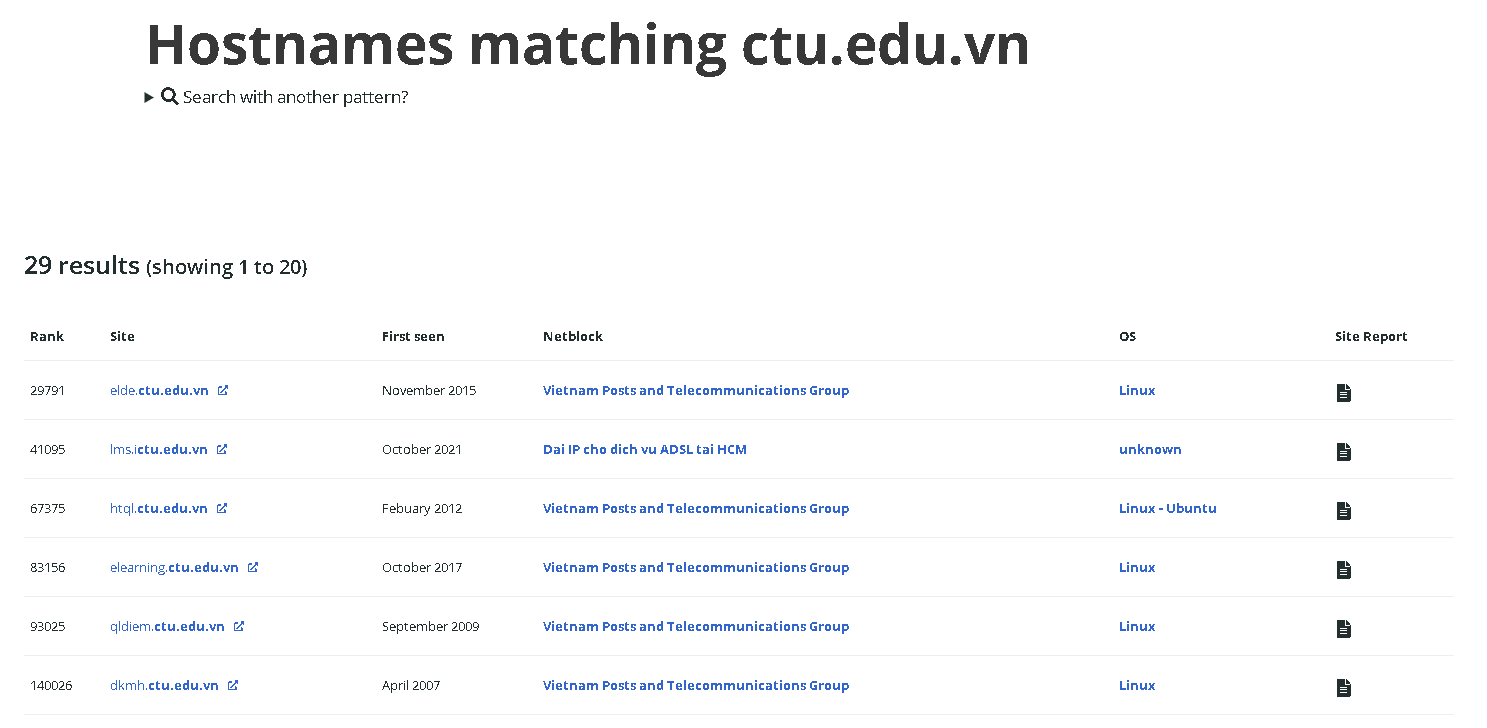
Identify web technologies used on CIT website

1. Search various information about the OS of the target using netcraft and explain the result.

<https://sitereport.netcraft.com/>



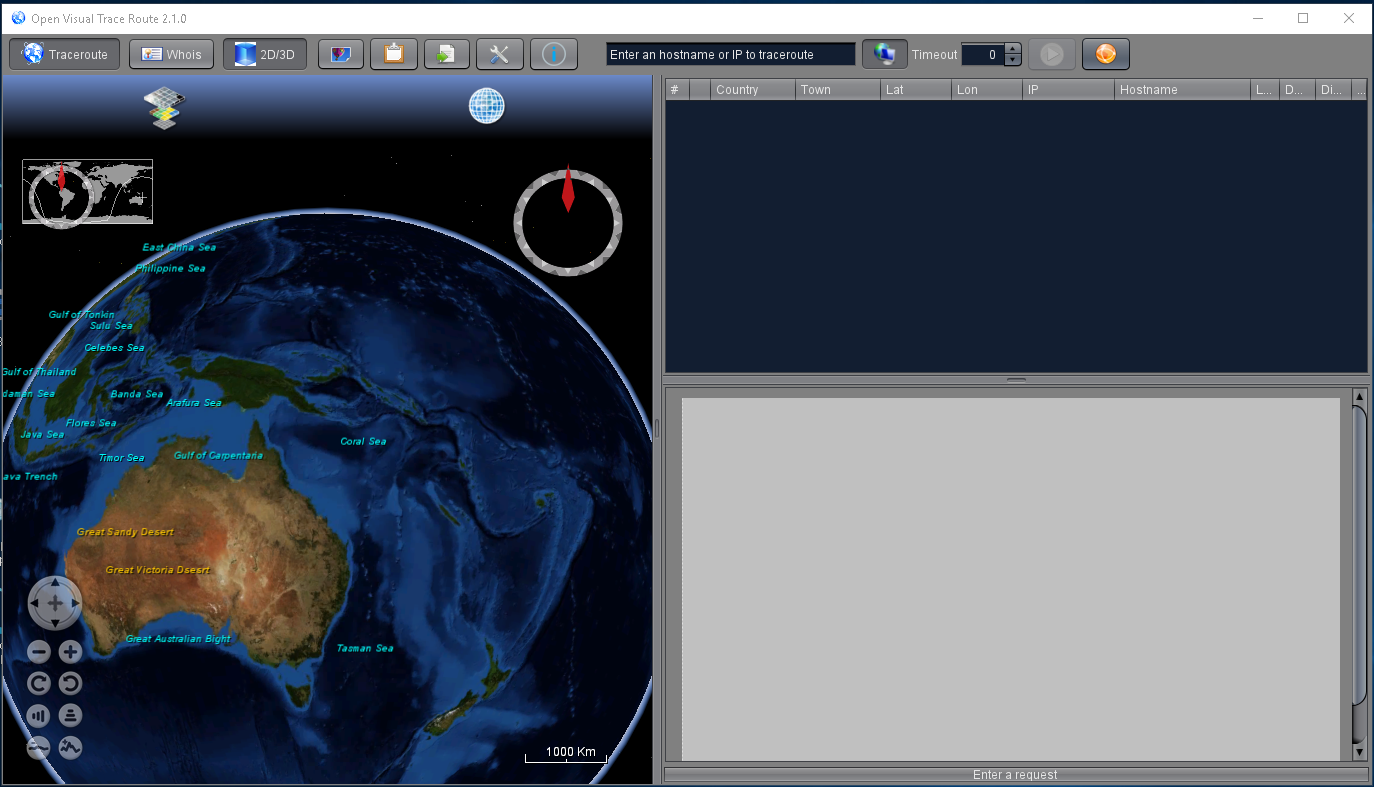
Web technologies of E-learning of CTU



Search hostnames matching \*ctu.edu.vn

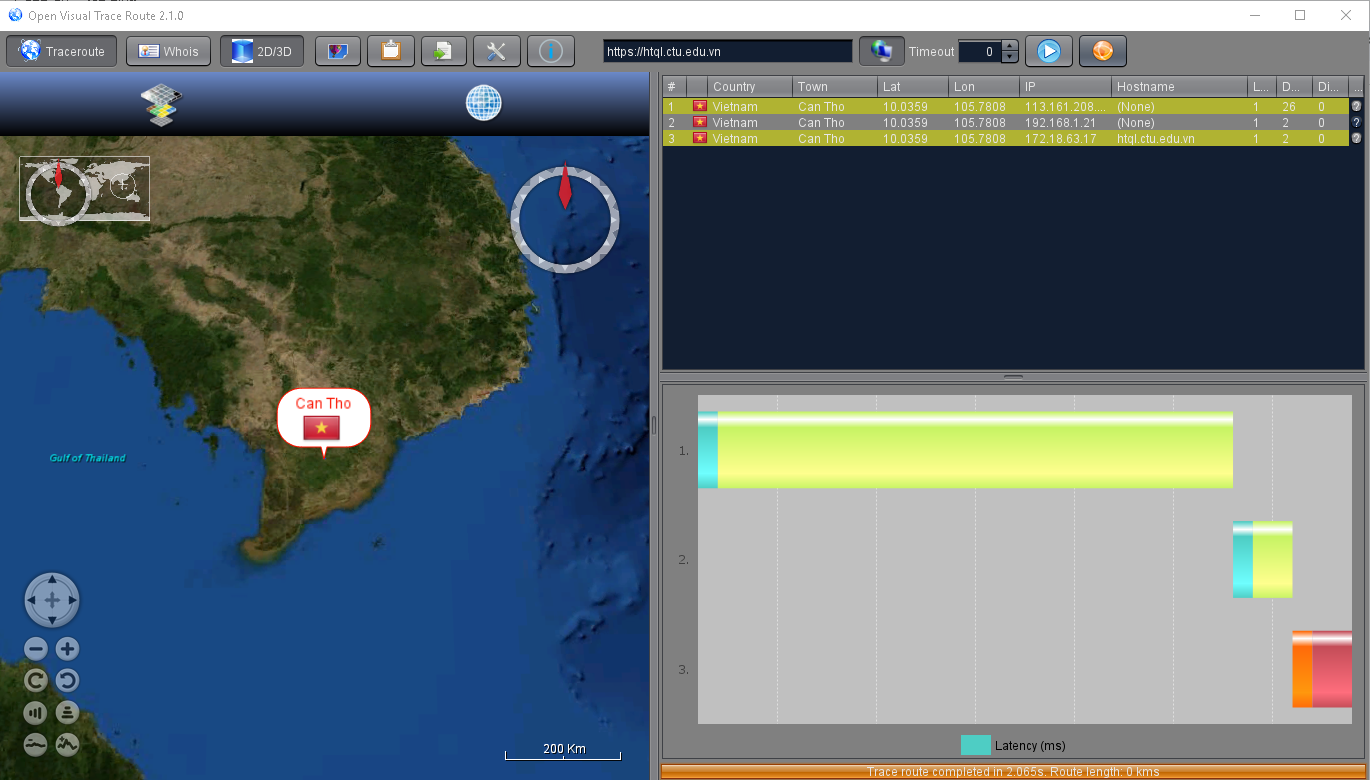
1. Download Open visual traceroute and execute

<https://sourceforge.net/projects/openvisualtrace/>



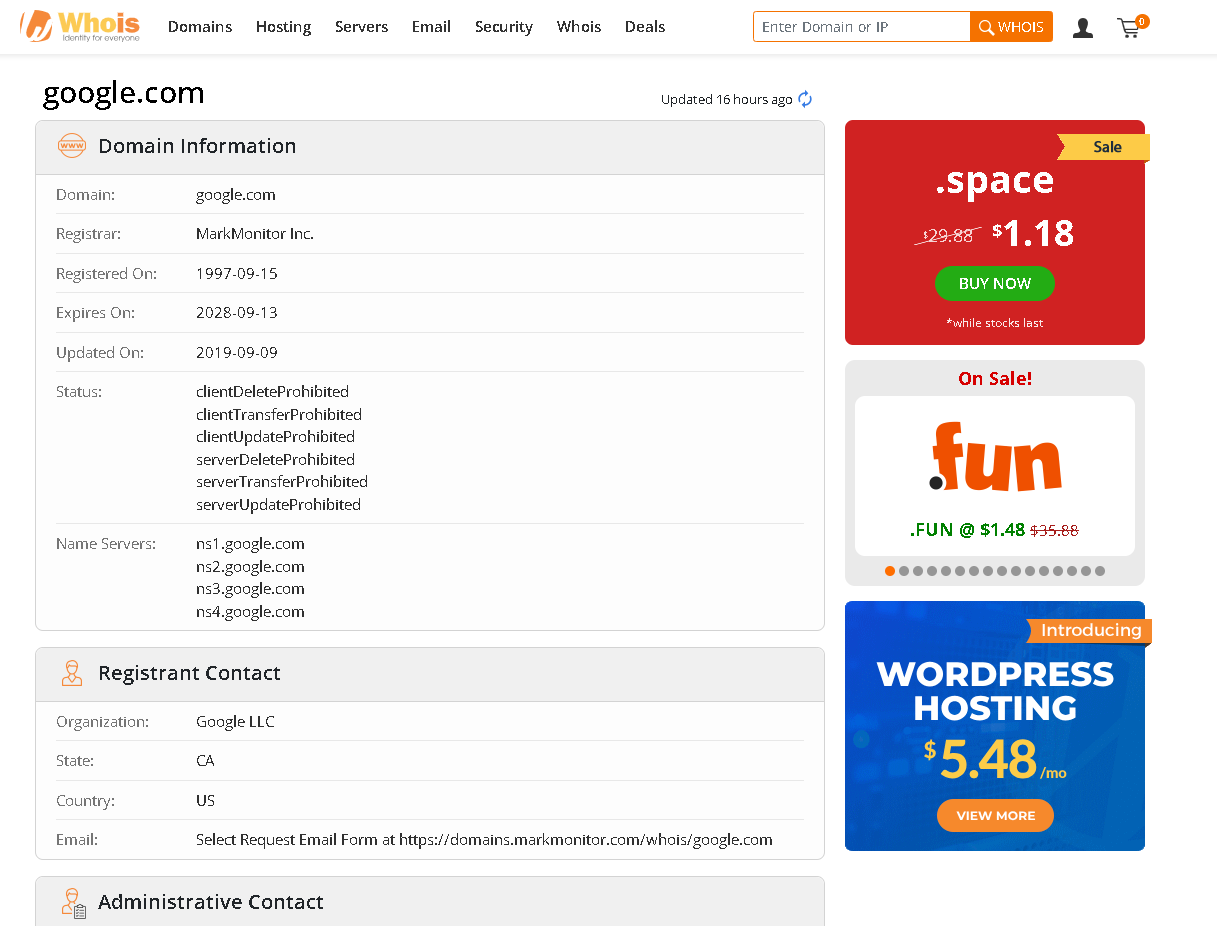
Download Open visual traceroute and execute

1. Test run Traceroute to target system and explain the test result.



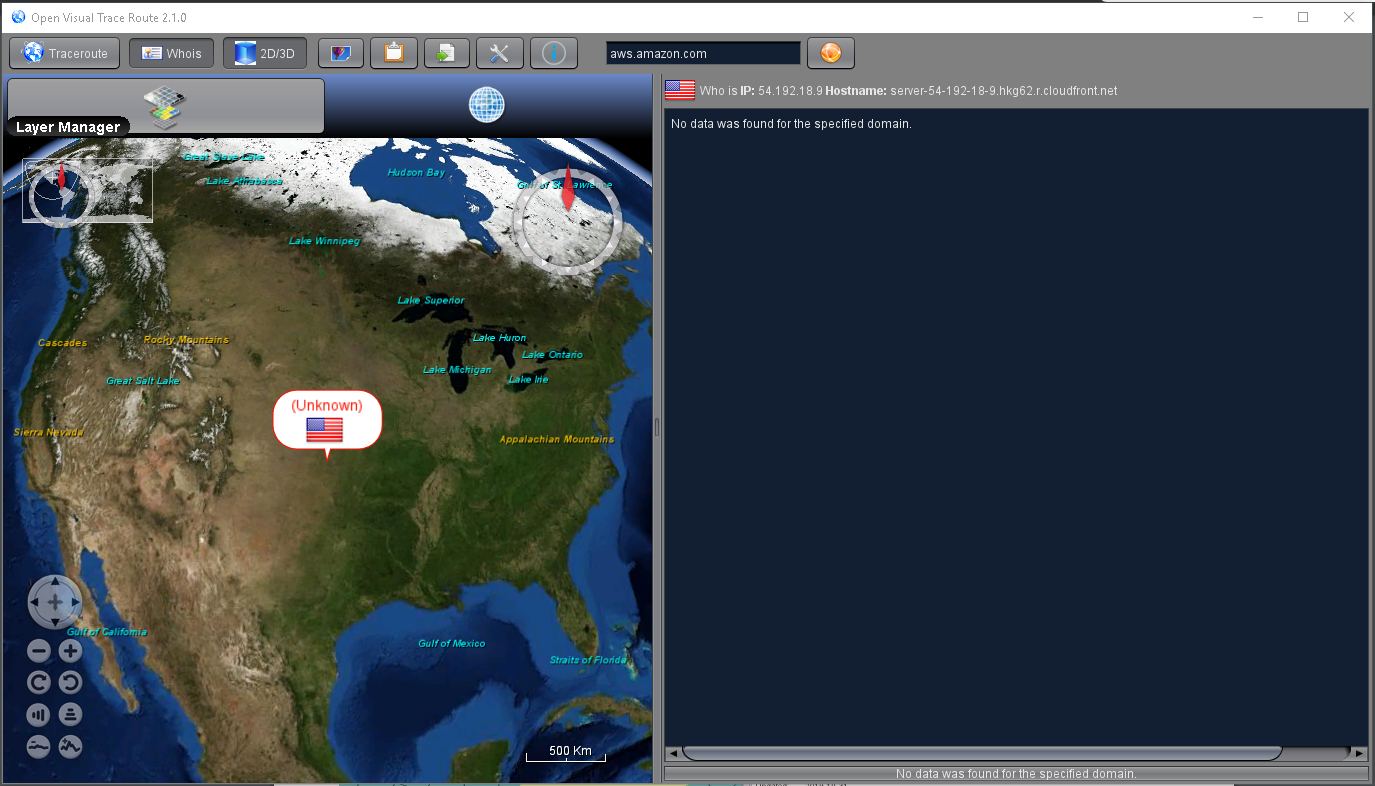
The traceroute test shows a successful, low-latency connection to htql.ctu.edu.vn in Can Tho, Vietnam, with minimal hops and efficient routing.

1. Test Whois to target the system and explain the test result.



Result when target Google

1. Test Whois 2D/3D Maps to target the system and explain the test result.

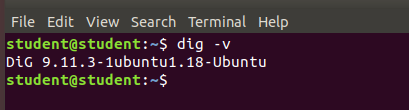


However I cannot test Whois with Open Visual Trace Route

**[model B]**

1. Install the dig command package utility, run and explain

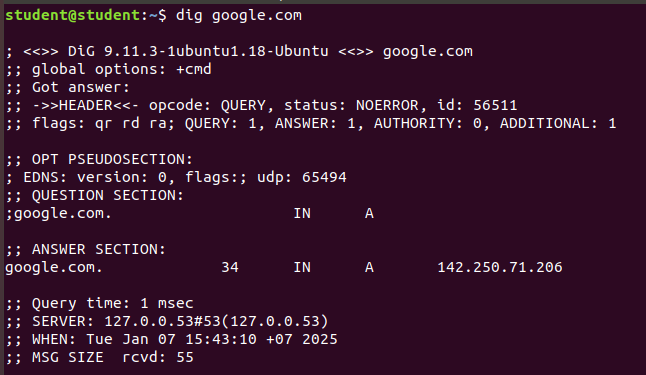
<https://linux.die.net/man/1/dig>



Installed Dig

1. Domain lookup

# dig google.com



The dig command successfully resolved google.com to   
the IP address 142.250.71.206 in 1 ms using the local DNS server at 127.0.0.53.

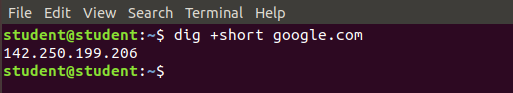
1. DNS lookup by specific name server

# dig @8.8.8.8 google.com

  
The dig command queries Google's public DNS (8.8.8.8) for   
the IP address of google.com, returning a successful response with the IP 142.250.199.78.

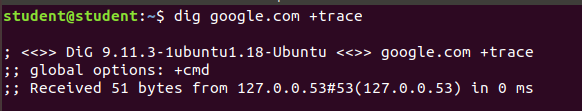
1. View response part only

# dig +short google.com

  
Shortly return a successful response with the IP 142.250.199.78.

1. DNS query tracking

# dig google.com +trace

  
Return the Traceroute

1. MX record verification

The mx option is an option to check if mx (mail record) is properly set.

# dig mx google.com

  
Google.com mail record is properly set.

**[model C]**

1. Visit Samspade site

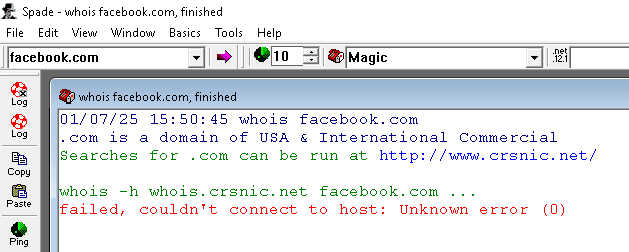
<https://www.majorgeeks.com/files/details/sam_spade.html>

1. Download Samspade



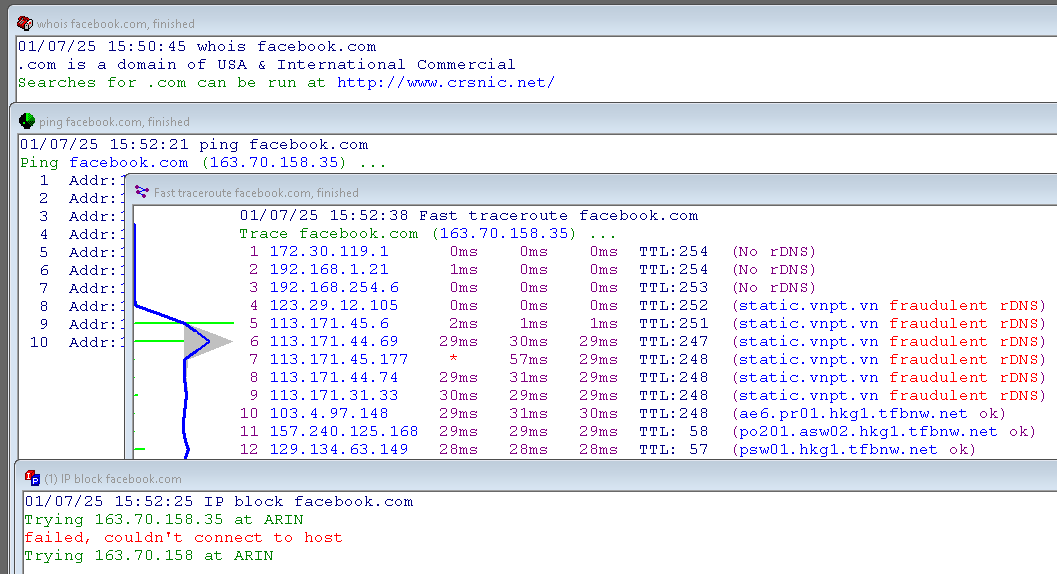


1. Input Target IP or URL in first box



Input facebook.com

1. Test Ping • Nslookup • Whois • ipblock • tracertroute • finger • Time • blacklist and explain the test result



It’s the same result as model A (with visualization)