Traceroute and Network Traffic Analysis

Written by Tyler Weiss 20 FEB 2024

Assignment

For this assignment you will be exploring the pathway your network traffic takes to reach an internet domain, using the CLI.

The aim of this exercise is to help you identify the various network routes your data packets travel through to reach google.com. You will also summarize these network routes, highlighting the journey from your local machine to the destination server. Further, this assignment will enable you to analyze how data traverses through different geographical locations and servers in route to its final destination.

Your submission should include a screenshot that captures the process you used to trace the route to google.com using the Traceroute command. Alongside the screenshot, provide a detailed explanation articulating in your own words the command(s) you utilized and their specific functions. This explanation should not only describe the technical steps undertaken but also offer insights into your understanding of how network routes are established and the significance of the various servers and geographical locations encountered during the data packet's journey.

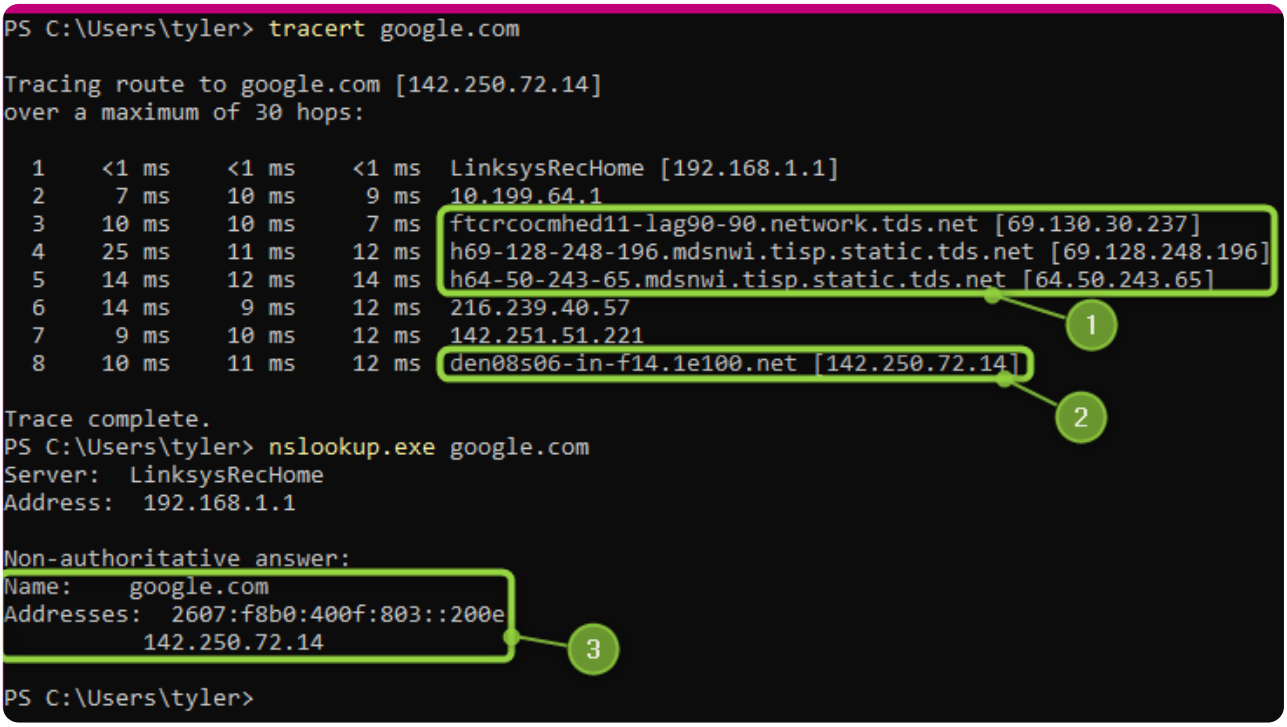
Exercise

The `tracert` command will report the route taken to a specified destination; either and IP address or a URL. The first column is the hop count to the destination in sequence. The center columns display the round trip time in milliseconds and represents network latency. The far right column is the address of each device a packet passes through to reach it's destination. So by tracing the route to `google.com` it's observed that:

1. the first hop is the network gateway. Following that the packet traverses the internet service providers nodes eventually moving outside of that network. This example

machine is using TDS as it's service provider.

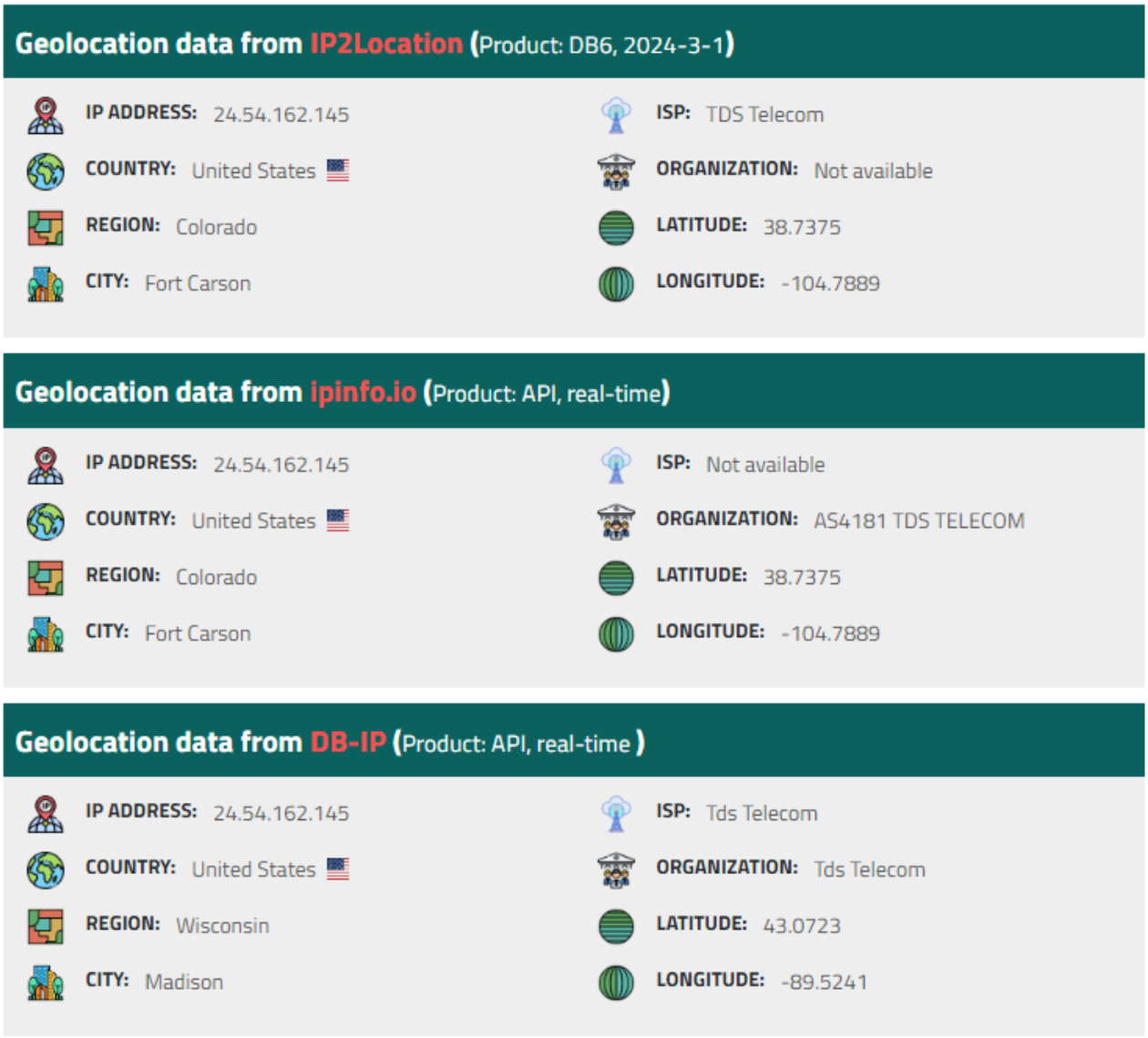
2. Finally the packet reaches it's destination at `google.com`.
3. The command `nslookup` queries the DNS record to resolve IP addresses and hostnames. In this example `nslookup google.com` is used to verify the destination address of the previous `tracert google.com` command.



The address `10.199.64.1` should be within the ISP's network and is probably with the local geographic area. Using `nslookup` will not resolve the IP address to a domain name because there isn't one for that particular node. A free online tool to perform an IP lookup should be available simply by searching 'ip address lookup' in your search engine. This example is uses https://www.iplocation.net/ip-lookup. The search results show that the address is indeed owned by TDS and is probably

located in Colorado.

Warning: 10.199.64.1 is a private IP address.



Using the previous method the other two IP address location and owner can be resolved. The below results show that `142.251.51.221` and `216.239.40.57` are owned by google and bridge between California and Colorado.

Geolocation data from IP2Location (Product: DB6, 2024-3-1)

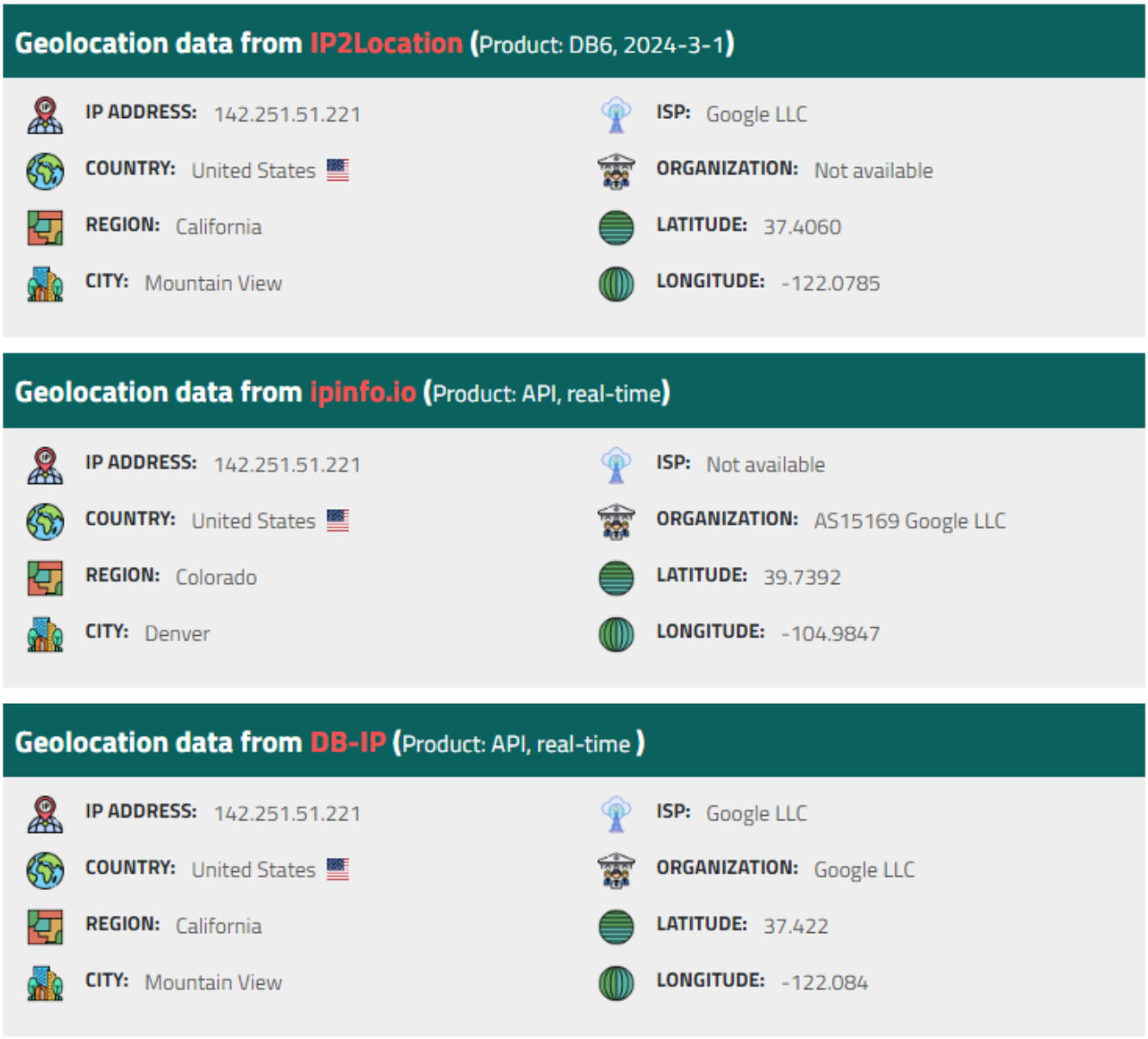
IP ADDRESS: 216.239.40.57
COUNTRY: United States
REGION: California
CITY: Mountain View
ISP: Google LLC
ORGANIZATION: Not available
LATITUDE: 37.4060
LONGITUDE: -122.0785

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 216.239.40.57
COUNTRY: United States
REGION: Colorado
CITY: Denver
ISP: Not available
ORGANIZATION: AS15169 Google LLC
LATITUDE: 39.7392
LONGITUDE: -104.9847

Geolocation data from DB-IP (Product: API, real-time)

IP ADDRESS: 216.239.40.57
COUNTRY: United States
REGION: California
CITY: Mountain View
ISP: Google LLC
ORGANIZATION: Google LLC
LATITUDE: 37.422
LONGITUDE: -122.084



These results prove that traffic flows from the local area network to the service provider and finally to the destination servers. It should also noted that the route to a destination will not always be the same. Routers on the network will attempt to take the least time-

consuming, or costly, route.

```
PS C:\Users\tyler> tracert google.com

Tracing route to google.com [142.250.72.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  LinksysRecHome [192.168.1.1]
  2     9 ms     7 ms     8 ms  10.199.64.1
  3     7 ms     7 ms     7 ms  ftcrcocmhed11-lag90-90.network.tds.net [69.130.30.237]
  4    12 ms    12 ms    12 ms  h69-128-248-196.mdsnwi.tisp.static.tds.net [69.128.248.196]
  5    13 ms    12 ms    13 ms  h64-50-243-65.mdsnwi.tisp.static.tds.net [64.50.243.65]
  6    12 ms    12 ms    12 ms  216.239.40.59
  7    12 ms    11 ms    12 ms  172.253.75.177
  8    12 ms    11 ms    10 ms  den16s08-in-f14.1e100.net [142.250.72.46]

Trace complete.
PS C:\Users\tyler>
```