

## 430/530 - Traceroute Lab

Answer the following questions using complete sentences. You may use outside sources to help you formulate responses; however, all answers should be in your own words, and sources should be cited.

### DNS Query Activity

	Original Website URL	Original Website IP Address	Discovered IP Address	Machine Name of Discovered IP
Example	www.google.com	172.217.6.4	172.217.6.36	sfo03s08-in-f4.1e100.net.
1	ipv4flagday.net	172.67.169.116	None Found	N/A
2	github.com	140.82.112.3	140.82.112.6	lb-140-82-112-6-iad.github.com.
3	www.mozilla.org	108.157.137.198	108.157.137.81	server-108-157-137-81.mci50.r.cloudfront.net.
4	wttr.in	5.9.243.187	5.9.243.225	static.225.243.9.5.clients.your-server.de.
5	www.freshports.org	54.227.255.74	54.227.255.99	ec2-54-227-255-99.compute-1.amazonaws.com.

Screen Capture – DNS query

```
> drill github.com
;; -->HEADER<-- opcode: QUERY, rcode: NOERROR, id: 42237
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; github.com. IN A
;; ANSWER SECTION:
github.com. 60 IN A 140.82.114.3
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;; Query time: 61 msec
;; SERVER: 8.8.8.8
;; WHEN: Thu Sep 29 10:44:06 2022
;; MSG SIZE rcvd: 44
> jboicken
```

Screen Capture – Reverse DNS query

```
> drill -x 140.82.112.6
;; -->HEADER<-- opcode: QUERY, rcode: NOERROR, id: 63906
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; 6.112.82.140.in-addr.arpa. IN PTR
;; ANSWER SECTION:
6.112.82.140.in-addr.arpa. 2315 IN PTR lb-140-82-112-6-iad.github.com.
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;; Query time: 54 msec
;; SERVER: 8.8.8.8
;; WHEN: Thu Sep 29 10:44:35 2022
;; MSG SIZE rcvd: 87
> jboicken
```

Q1: Attacker using nslookup/dig

An attacker can use dns lookups to perform reconnaissance. They can use dig to find machines, if the DNS server gives a PTR response that means that IP address is being used by a machine.

# Packet Routing

## Screen Capture – traceroute/tracert

```
> traceroute -m 20 amazon.com
traceroute: Warning: amazon.com has multiple addresses; using 52.94.236.248
traceroute to amazon.com (52.94.236.248), 20 hops max, 40 byte packets
 1 * * *
 2 10.33.137.252 (10.33.137.252) 28.783 ms 6.663 ms 5.826 ms
 3 b31-mpls-p-hu0-2-0-2--to--b31-mpls-pe-wifi1-1-0-51.tele.iastate.edu (129.186.0.148) 6.465 ms 5.005 ms 5.546 ms
 4 b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135) 8.870 ms
   e63-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.137) 6.637 ms
   b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135) 5.967 ms
 5 b31fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.247) 5.093 ms 6.258 ms
   b31fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.255) 5.742 ms
 6 e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231) 6.357 ms
   b31be-eth1-2.fusion.tele.iastate.edu (192.188.159.227) 6.000 ms 6.777 ms
 7 rtr-b31nat1-vlan920.tele.iastate.edu (192.188.159.132) 5.804 ms 4.859 ms 16.376 ms
 8 rtr-b31be1-vlan931.tele.iastate.edu (192.188.159.177) 5.566 ms 6.544 ms 6.374 ms
 9 rtr-b31isp1-be152.tele.iastate.edu (192.188.159.153) 6.331 ms 15.650 ms 6.054 ms
10 164.113.254.205 (164.113.254.205) 11.194 ms 12.458 ms 15.066 ms
11 amazon.gnd1.mci.kcix.net (206.51.7.131) 12.958 ms 13.436 ms 12.738 ms
12 15.230.183.74 (15.230.183.74) 12.139 ms
   15.230.183.62 (15.230.183.62) 16.832 ms
   15.230.183.50 (15.230.183.50) 16.099 ms
13 * * *
14 15.230.183.124 (15.230.183.124) 25.663 ms
   15.230.183.104 (15.230.183.104) 11.273 ms
   15.230.183.120 (15.230.183.120) 13.124 ms
15 15.230.183.69 (15.230.183.69) 11.633 ms
   15.230.183.55 (15.230.183.55) 12.930 ms
   15.230.183.37 (15.230.183.37) 14.500 ms
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
```

Q2: \* \* \* traceroute results

The \*\*\* is shown when the router does not respond in a certain amount of time. A router could simply be programmed to not respond to TTL or a firewall may block the ICMP response. Another possibility is network congestion prevents the packet from reaching the sender in the time period.

## Network Diagram

Answer the following questions from the lab using complete sentences.

Q3: traceroute/tracert output

I don't think traceroute would display the route. There is no guarantee by IP to send packets in the same route. Depending upon network congestion and changes to network between the two end devices, the packets could very easily be sent on a different path than what was shown.

Q4: Geographical location

<https://stackoverflow.com/questions/1996106/how-does-ip-geolocating-work>.

<https://whatismyipaddress.com/geolocation>.

This stackoverflow and my ip pages show that geolocation services have a large database of information that is used to correlate an IP and webpage to a location. They use the registry and ISPs to get information on where the IP is. As well, they can use information on who is hosting the webpage to learn where it is like iastate is Ames or something in AWS is only where there are databases physically. Which is known information. This only gets so close to where something is like to the city and only if they are stored in their database.

Q5: Routers in the network

1

Q6: Dynamic routing

Yes, there is dynamic routing in the diagram. The jump after 192.188.159.227 has multiple choices to either 192.188.159.132 or 192.188.159.152 that we see in the traceroutes. The hops after both of those go to the same point so we know of multiple possible paths that can be taken dynamically.

Upload your network diagram here.

