Homework#4

1. (5 points) Find out the exact number of all top domain names. Make sure you put a date and time of your finding. (Hint: use the information given at the lecture to locate the list of names at IANA.)

Solution:

There are **1516** top domain names as of March 13, 2020 Eastern Time 11:24 am.

Source: [http://data.iana.org/TLD/tlds-alpha-by-domain.txt]

2. (5 points) Experiment with http://whois.domaintools.com (and also take a look at www.internic.net) and

a. Find the information about the stevens.edu domain as well as the domain of some other school (for instance, the school you had studied at before you came to Stevens). Who are the administrative contacts for the domains listed there?

Solution:

Registrant Org	Stevens Institute of Technology
Dates	7,932 days old
	Created on 1998-06-25
	Expires on 2022-07-31
Tech Contact	Domain Name Administration
IP Address	104.16.125.51 is hosted on a dedicated server
IP Location	California – San Francisco Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
IP History	12 changes on 12 unique IP addresses over 15 years
Hosting History	4 changes on 3 unique name servers over 18 years
Domain	stevens.edu
Server Type	cloudflare

*Stevens information is not available on internic.net

For my undergrad school: SGGSIET

Registrant Org	Shri Guru Govind Singhji Institute of Engineering and Technology
Registrant Country	in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in
Dates	6,124 days old Created on 2003-06-07 Expires on 2028-06-07 Updated on 2019-05-17
Name servers	NS1.CS-MUM-25.BIGROCKSERVERS.COM (has 47,525 domains) NS2.CS-MUM-25.BIGROCKSERVERS.COM (has 47,525 domains)
Tech Contact	
IP Address	103.76.228.18 - 295 other sites hosted on this server
IP Location	Karnataka - Mangalore - Endurance Web Solutions Private Limited
ASN	AS394695 PUBLIC-DOMAIN-REGISTRY, US (registered Nov 24, 2015)
Server Type	Apache/2.4.39 (cPanel) OpenSSL/1.0.2r mod_bwlimited/1.4 Phusion_Passenger/5.3.7

Source: [https://reports.internic.net/cgi/whois?whois_nic=103.76.228.18&type=nameserver] [http://whois.domaintools.com/sggs.ac.in] [http://whois.domaintools.com/stevens.edu]

b. Now, what happens when you try to find the administrative contact for the .xxx

domain? Explain what you have found.

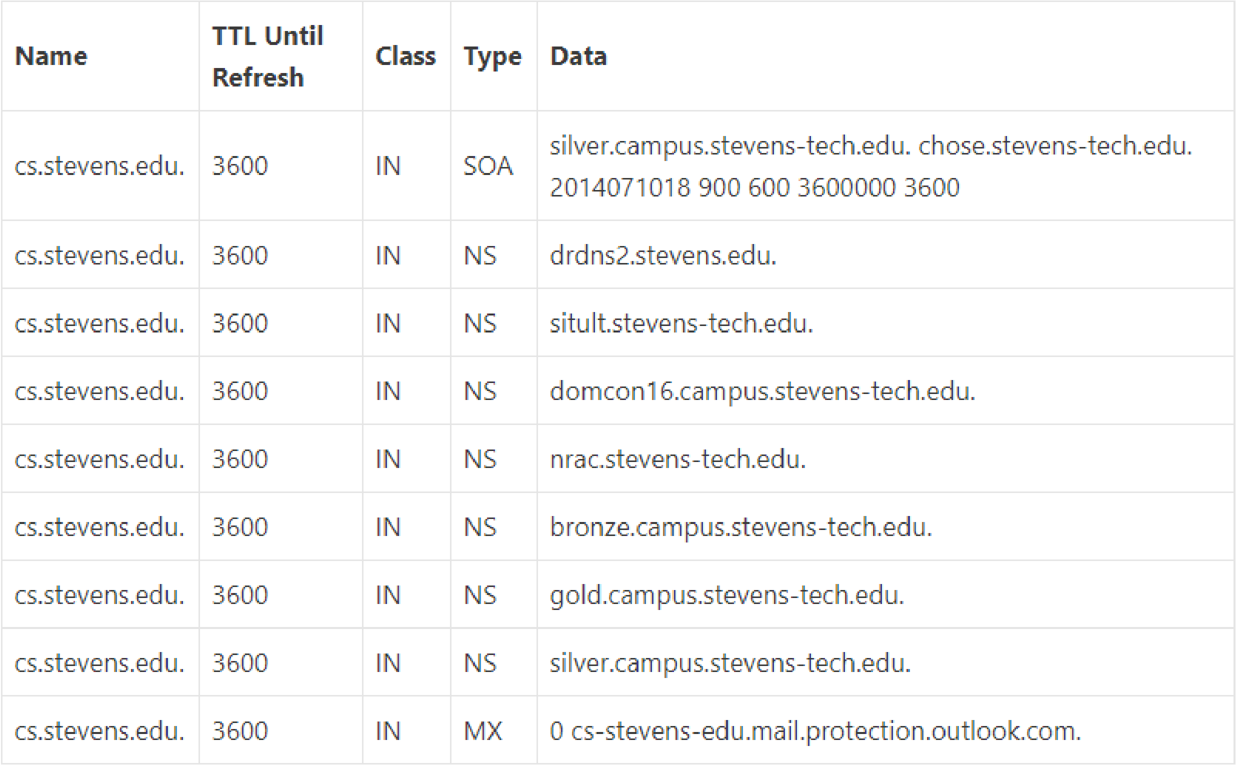
Solution: The .xxx domain has Registration Private as the Registrant and the registrant organization is Domains by Proxy, LLC. It's tech contact is By Proxy, LLC, Domains ByProxy.com, Scottsdale, Arizona, 85260, US. It is a domain for Adult Community. The following is its admin contact details:

Admin Contact
ICM Registry LLC
2505 Second Ave, Suite 520
Seattle, Washington 98121
United States
Email: ops@mmx.co
Voice: +1 877 734 4783
Fax: +1 877 809 3183

Source: [https://www.iana.org/domains/root/db/xxx.html]

3. (5 points) Look up www.cs.stevens.edu https://network-tools.com/nslookup/ with different options and explain all the entries in the responses.
Then use the returned CNAME entry to find the exact IP address. (Now, just for fun, do the reverse DNS lookup using the services of the http://dnsquery.org and find the geographic location of the host!)
Does Stevens specify IPV6 addresses to any of its hosts? Does Google?

Solution:



Name	TTL Until Refresh	Class	Type	Data
cs.stevens.edu.	3600	IN	SOA	silver.campus.stevens-tech.edu. chose.stevens-tech.edu. 2014071018 900 600 3600000 3600
cs.stevens.edu.	3600	IN	NS	drdns2.stevens.edu.
cs.stevens.edu.	3600	IN	NS	sitult.stevens-tech.edu.
cs.stevens.edu.	3600	IN	NS	domcon16.campus.stevens-tech.edu.
cs.stevens.edu.	3600	IN	NS	nrac.stevens-tech.edu.
cs.stevens.edu.	3600	IN	NS	bronze.campus.stevens-tech.edu.
cs.stevens.edu.	3600	IN	NS	gold.campus.stevens-tech.edu.
cs.stevens.edu.	3600	IN	NS	silver.campus.stevens-tech.edu.
cs.stevens.edu.	3600	IN	MX	0 cs-stevens-edu.mail.protection.outlook.com.

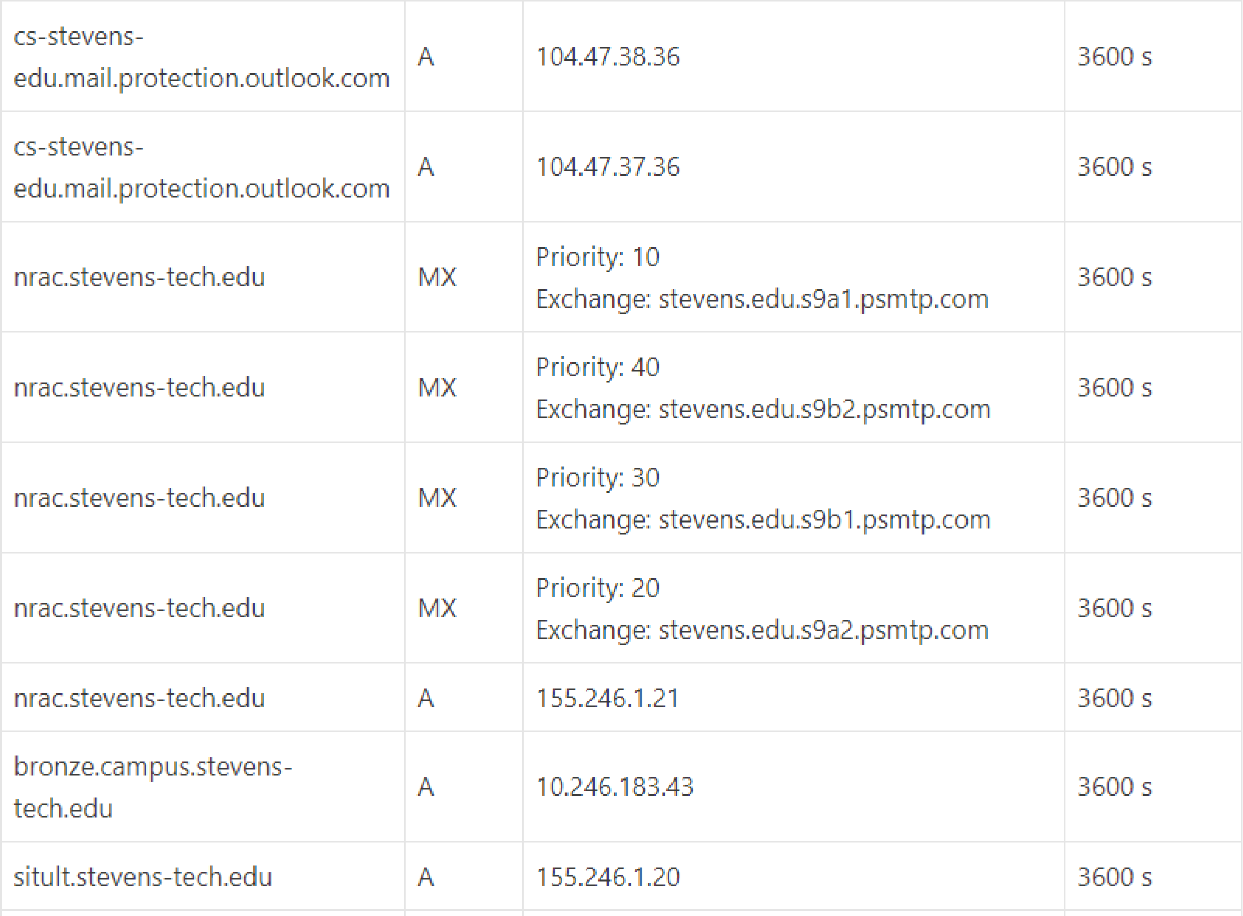
Name: The name of the domain to lookup for.
TTL Until Refresh: TTL stands for “Time to Live” and it refers to how long your DNS settings are supposed to be cached before they are automatically refreshed.
Class: IN stands for Internet
Type: DNS servers create a DNS record to provide important information about a domain or hostname, particularly its current IP address. The most common DNS record types are:

- Start of Authority (SOA Record)—this record appears at the beginning of a DNS zone file, and indicates the Authoritative Name Server for the current DNS zone, contact details for the domain administrator, domain serial number, and information on how frequently DNS information for this zone should be refreshed.
- Name Server records (NS Record)—specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server.

- Mail exchanger record (MX Record)—specifies an SMTP email server for the domain, used to route outgoing emails to an email server.

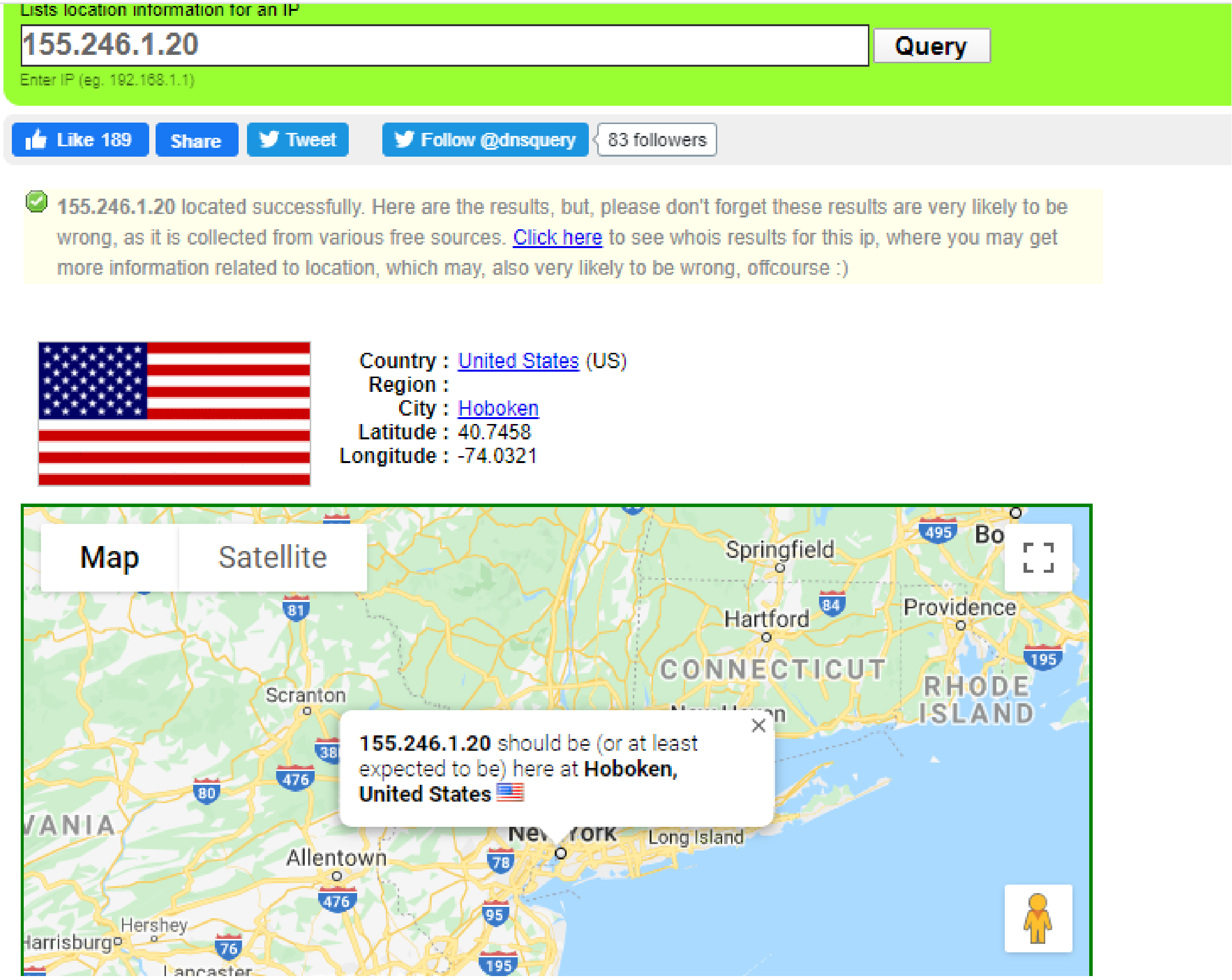
Data: DNS is a client-server-system: a kind of digital "phone book" with DNS data.

Since there are no CNAME records, the additional records are:



cs-stevens-edu.mail.protection.outlook.com	A	104.47.38.36	3600 s
cs-stevens-edu.mail.protection.outlook.com	A	104.47.37.36	3600 s
nrac.stevens-tech.edu	MX	Priority: 10 Exchange: stevens.edu.s9a1.psmtp.com	3600 s
nrac.stevens-tech.edu	MX	Priority: 40 Exchange: stevens.edu.s9b2.psmtp.com	3600 s
nrac.stevens-tech.edu	MX	Priority: 30 Exchange: stevens.edu.s9b1.psmtp.com	3600 s
nrac.stevens-tech.edu	MX	Priority: 20 Exchange: stevens.edu.s9a2.psmtp.com	3600 s
nrac.stevens-tech.edu	A	155.246.1.21	3600 s
bronze.campus.stevens-tech.edu	A	10.246.183.43	3600 s
sitult.stevens-tech.edu	A	155.246.1.20	3600 s

Reverse Lookup for Ip Address 155.246.1.20 gives:



Lists location information for an IP

155.246.1.20 Query

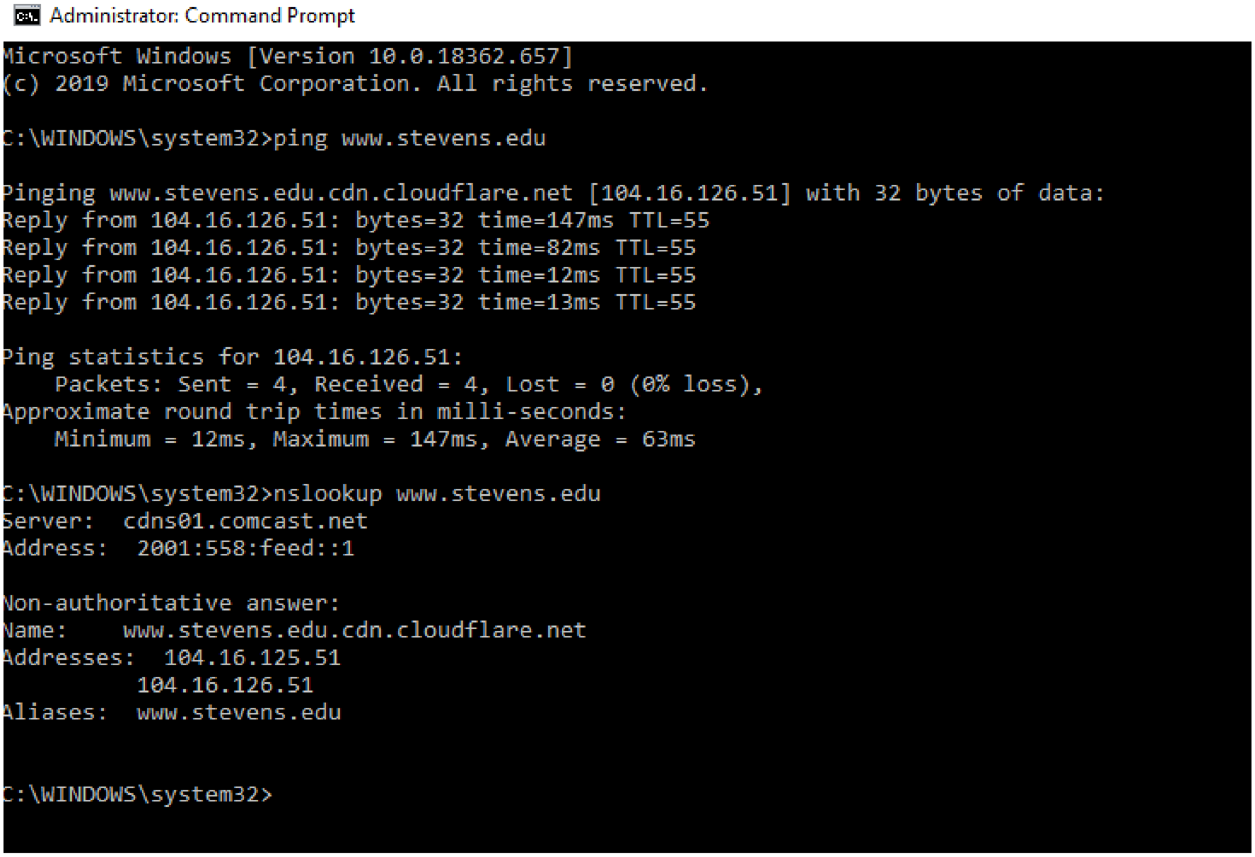
Enter IP (eg. 192.168.1.1)

155.246.1.20 located successfully. Here are the results, but, please don't forget these results are very likely to be wrong, as it is collected from various free sources. Click here to see whois results for this ip, where you may get more information related to location, which may, also very likely to be wrong, offcourse :)

Country : United States (US)
Region :
City : Hoboken
Latitude : 40.7458
Longitude : -74.0321

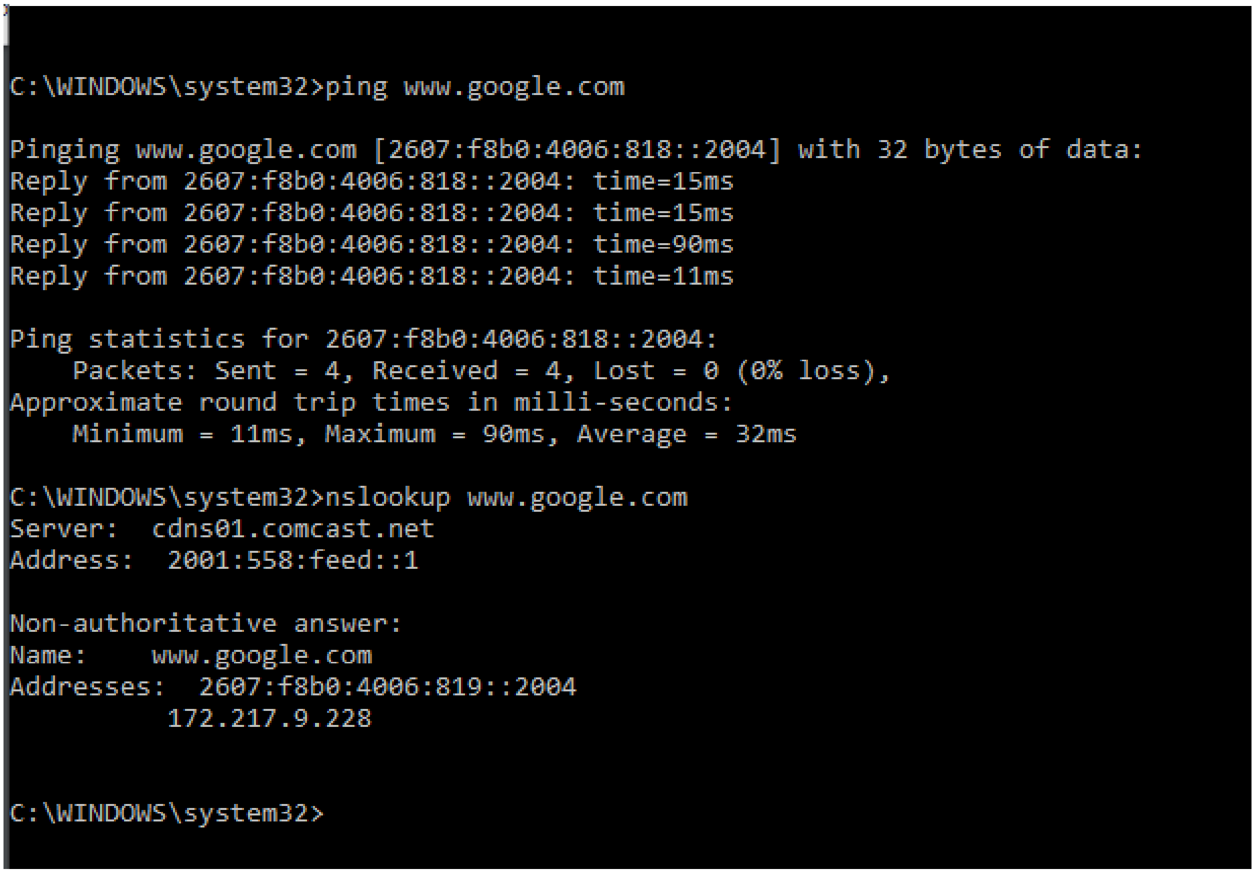
155.246.1.20 should be (or at least expected to be) here at **Hoboken, United States**

No, Stevens does not specifies IPv6 addresses to any of its hosts.



```
Microsoft Windows [Version 10.0.18362.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.stevens.edu

Pinging www.stevens.edu.cdn.cloudflare.net [104.16.126.51] with 32 bytes of data:
Reply from 104.16.126.51: bytes=32 time=147ms TTL=55
Reply from 104.16.126.51: bytes=32 time=82ms TTL=55
Reply from 104.16.126.51: bytes=32 time=12ms TTL=55
Reply from 104.16.126.51: bytes=32 time=13ms TTL=55

Ping statistics for 104.16.126.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 147ms, Average = 63ms

C:\WINDOWS\system32>nslookup www.stevens.edu
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    www.stevens.edu.cdn.cloudflare.net
Addresses:  104.16.125.51
          104.16.126.51
Aliases:  www.stevens.edu


C:\WINDOWS\system32>
```

Yes, Google specifies IPv6 addresses to its hosts.

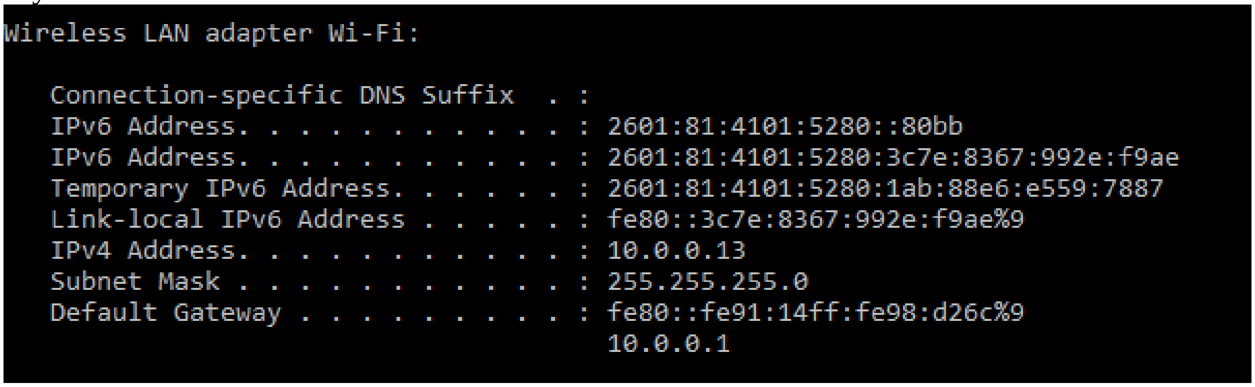


```
C:\WINDOWS\system32>ping www.google.com

Pinging www.google.com [2607:f8b0:4006:818::2004] with 32 bytes of data:
Reply from 2607:f8b0:4006:818::2004: time=15ms
Reply from 2607:f8b0:4006:818::2004: time=15ms
Reply from 2607:f8b0:4006:818::2004: time=90ms
Reply from 2607:f8b0:4006:818::2004: time=11ms

Ping statistics for 2607:f8b0:4006:818::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 90ms, Average = 32ms

C:\WINDOWS\system32>nslookup www.google.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:4006:819::2004
          172.217.9.228


C:\WINDOWS\system32>
```

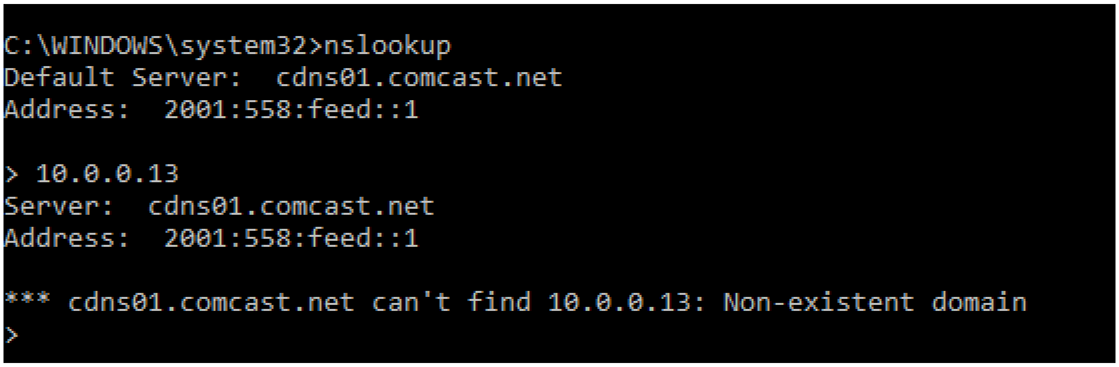
Source: [https://ns1.com/resources/dns-types-records-servers-and-queries#:~:text=DNS%20servers%20create%20a%20DNS,and%20its%20corresponding%20IPv4%20address.] [https://network-tools.com/nslookup/]

4. (5 points) Find your PC’s IP address (preferably at home, if you have an Internet connection there.) Can you find your domain with the reverse look up? If you can, what is the domain name? If you cannot, explain why.

Solution:
My PC’s IP address is 10.0.0.13



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2601:81:4101:5280::80bb
   IPv6 Address. . . . . . . . . . . : 2601:81:4101:5280:3c7e:8367:992e:f9ae
   Temporary IPv6 Address. . . . . . : 2601:81:4101:5280:1ab:88e6:e559:7887
   Link-local IPv6 Address . . . . . : fe80::3c7e:8367:992e:f9ae%9
   IPv4 Address. . . . . . . . . . . : 10.0.0.13
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::fe91:14ff:fe98:d26c%9
                                       10.0.0.1
```



```
C:\WINDOWS\system32>nslookup
Default Server:  cdns01.comcast.net
Address:  2001:558:feed::1

> 10.0.0.13
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

*** cdns01.comcast.net can't find 10.0.0.13: Non-existent domain
>
```

The addresses 10.0.0.0 - 10.255.255.255 are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
A NXDOMAIN is Non-Existent Domain. It is a term used for the Internet domain name that is unable to be resolved using the DNS servers or domain name not yet registered. NXDOMAIN can also take place due to the network or DNS server problem.

Source: [http://whois.domaintools.com/10.0.0.13]

5. (10 points) Research the responsibilities and structure of IANA (www.iana.com) and ICANN (www.icann.com). What are the differences in responsibilities between these two organizations? Search the web for the information and then describe the controversy in ICANN concerning Whois?

Solution:
IANA: The Internet Assigned Numbers Authority (IANA) is a function of ICANN, a nonprofit private American corporation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and Internet numbers.

- IANA is responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.
- Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet.
- IANA's various activities can be broadly grouped in to three categories:
    - ✓ Domain Names: Management of the DNS Root, the .int and. arpa domains, and an IDN practices resource.
    - ✓ Number Resources: Co-ordination of the global pool of IP and AS numbers, primarily providing them to Regional Internet Registries (RIRs).
    - ✓ Protocol Assignments: Internet protocols' numbering systems are managed in conjunction with standards bodies.

ICANN: The Internet Corporation for Assigned Names and Numbers (ICANN) is an American multi-stakeholder group and nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation.

To reach another person on the Internet you have to type an address into your computer -- a name or a number. That address must be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination, we wouldn't have one global Internet. In more technical terms, the Internet Corporation for Assigned Names and Numbers (ICANN) helps coordinate the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS).

The IANA functions include:

(1) the coordination of the assignment of technical protocol parameters including the management of the address and routing parameter area (ARPA) top-level domain;

(2) the administration of certain responsibilities associated with Internet DNS root zone management such as generic (gTLD) and country code (ccTLD) Top-Level Domains;

(3) the allocation of Internet numbering resources; and

(4) other services.

IANA vs ICANN:

- ICANN is responsible for the centralization of registration tasks related to IP addresses, DNS assignment and protocol parameters management, but ICANN does not replace IANA.
- There are many differences between ICANN and IANA, especially regarding their attributions, objectives and responsibilities.
- IANA is the institution which runs TLDs (Top-Level Domains) and deals with the assignment of IP addresses and ranges, ports, and other related attributes.
- ICANN, based on the Memorandum of Understanding (MoU), is the institution which runs IANA.

WHOIS restriction Controversy:

- ✓ Intended to be a source of information about domain owners, WHOIS has become a lightning rod for controversy over the years, much of which is aimed at registrars and ICANN for failing to properly crack down on domain owners with inaccurate WHOIS data.
- ✓ WHOIS refers to the data directly related to a domain name, which includes a name, address, e-mail, phone number and other personal information.
- ✓ In anticipation of the now approved European General Data Protection Regulation (GDPR), the Internet Corporation for Assigned Names and Numbers (ICANN), an American organization tasked with accrediting registrars and enforcing WHOIS policies, approved a new and revised Temporary Specification for gTLD registration data to ensure its domain information policies meet the EU’s new data privacy rules.
- ✓ Limiting access to previously public data was met with disapproval by law enforcement agencies using WHOIS data to investigate cybercrimes.

- ✓ The International Trademark Association (INTA) protested the Temporary Specification by stating that restriction to WHOIS data will likely increase incidents involving online fraud and abuse.
- ✓ As a result, INTA is now asking stakeholders and IP practitioners worldwide to submit stories detailing the negative effects of restricting access to WHOIS data.
- ✓ According to INTA, limiting access to the domain name database "fundamentally challenges the way legal practitioners protect their brands." INTA members use the WHOIS database to track down individuals behind online counterfeiting, the distribution of malicious software and suspicious online behavior.
- ✓ ICANN's struggle with new EU data privacy legislation, however, was not resolved with the Temporary Specification. In late May, the US-based organization found itself in a tight spot after unsuccessfully filing an injunction which would force a German registrar to continue gathering people's data. Arguing that the required WHOIS data was non-essential to set up a domain and that such a request would go against data privacy rights, a German court ruled against the injunction.
- ✓ ICANN now faces pressure from both European data privacy regulators and international agencies such as INTA to regularize WHOIS data gathering and to make information about the individuals and businesses behind domain names public, all whilst complying with EU data privacy laws.

Source: [https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority] [https://www.iana.org/about] [https://en.wikipedia.org/wiki/ICANN] [https://www.securityweek.com/icanns-rolling-controversy-verification-whois-registration-data] [https://www.leadersleague.com/en/news/whois-restriction-sparks-controversy]

6. (50 points) The Spamhaus attack
a. (5 points) Read https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminalconspiracy-2/ . Describe (in no more than a couple of paragraphs) the Spamhaus attack and explain the dangers of open recursive resolvers.
b. (45 points) Find out (you will need to search the Web and sort a lot of information out!) how cloud services were used to mitigate this attack.

Solution:
a. **The Spamhaus attack:**

- ➢ Spamhaus provides one of the key backbones that underpins much of the anti-spam filtering online. Run by a tireless team of volunteers, Spamhaus patrols the Internet for spammers and publishes a list of the servers they use to send their messages in order to empower email system administrators to filter unwanted messages.
- ➢ Beginning on March 18, the Spamhaus site came under attack. The attack was large enough that the Spamhaus team wasn't sure of its size. It was sufficiently large to fully saturate their connection to the rest of the Internet and knock their site offline.
- ➢ These very large attacks, which are known as Layer 3 attacks, are difficult to stop with any on-premise solution. Put simply: if you have a router with a 10Gbps port, and someone sends you 11Gbps of traffic, it doesn't matter what intelligent software you have to stop the attack because your network link is completely saturated.

- A significant component of the DDOS traffic targeted at Spamhaus is coming from a technique that has been known for years – a variety of reflection attack commonly known as a "DNS amplification attack." By relying on the fact that an answer to a DNS query can be much larger than the query itself, attackers are able to both amplify the magnitude of the traffic directed against a DDOS victim and conceal the source of the attacking machines.

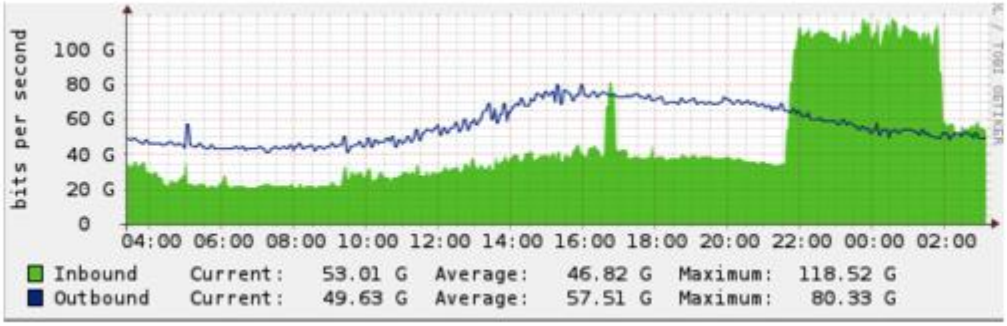
Dangers of Open-recursive resolvers:

- To accomplish an attack which was carried out on Spamhaus, the attacker sends a DNS query a few bytes in size to an open resolver, forging a "spoofed" source address for the query. The open resolver, believing the spoofed source address, sends a response which can be hundreds of bytes in size to the machine it believes originated the request. The end result is that the victim's network connection is hit with several hundred bytes of information that were not requested. They will be discarded when they reach the target machine, but not before exhausting a portion of the victim's network bandwidth. And the traffic reaching the victim comes from the open resolver, not from the machine or machines used to initiate the attack.
- Given a large list of open resolvers to reflect against, an attacker using a DNS amplification attack can hide the origin of their attack and magnify the amount of traffic they can direct at the victim by a factor of **40** or more.
- DNS operators who operate open resolvers without taking precautions to prevent their abuse generally believe they are harming nobody, but as the Spamhaus DDOS proves, open resolvers can be effortlessly coopted by attackers and used in criminal attacks on third parties.

Source: [https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/]
[https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/]

b. Mitigation of Spamhaus attack:

- Spamhaus signed up for CloudFlare and they immediately mitigated the attack, making the site once again reachable. Once on CloudFlare's network, they also began recording data about the attack. At first, the attack was relatively modest (around 10Gbps). There was a brief spike around 16:30 UTC, likely a test, that lasted approximately 10 minutes. Then, around 21:30 UTC, the attackers let loose a very large wave.
- The graph below is generated from bandwidth samples across a number of the routers that sit in front of servers CloudFlare uses for DDoS scrubbing. The green area represents in-bound requests and the blue line represents out-bound responses. While there is always some attack traffic on CloudFlare's network, it's easy to see when the attack against Spamhaus started and then began to taper off around 02:30 UTC on March 20, 2013. As of 16:15 UTC on March 20, 2013, the attack picked up again.



- The largest source of attack traffic against Spamhaus came from DNS reflection. In the Spamhaus case, the attacker was sending requests for the DNS zone file for ripe.net to open DNS resolvers. The attacker spoofed the CloudFlare IPs issued for Spamhaus as the source in their DNS requests. The open resolvers responded with DNS zone file, generating collectively approximately 75Gbps of attack traffic. The requests were likely approximately 36 bytes long (e.g. dig ANY ripe.net @X.X.X.X+edns=0 +bufsize=4096, where X.X.X.X is replaced with the IP address of an open DNS resolver) and the response was approximately 3,000 bytes, translating to a 100x amplification factor.
- CloudFlare recorded over 30,000 unique DNS resolvers involved in the attack. This translates to each open DNS resolver sending an average of 2.5Mbps, which is small enough to fly under the radar of most DNS resolvers. Because the attacker used a DNS amplification, the attacker only needed to control a botnet or cluster of servers to generate 750Mbps -- which is possible with a small sized botnet or a handful of AWS instances.
- While large Layer 3 attacks are difficult for an on-premise DDoS solution to mitigate, CloudFlare's network was specifically designed from the beginning to stop these types of attacks. They make heavy use of Anycast. That means the same IP address is announced from every one of their 23 worldwide data centers. The network itself load balances requests to the nearest facility. Under normal circumstances, this helps to ensure a visitor is routed to the nearest data center on their network.
- When there's an attack, Anycast serves to effectively dilute it by spreading it across their facilities. Since every data center announces the same IP address for any CloudFlare customer, traffic cannot be concentrated in any one location. Instead of the attack being many-to-one, it becomes many-to-many with no single point on the network acting as a bottleneck.
- Once diluted, the attack becomes relatively easy to stop at each of the data centers. Because CloudFlare acts as a virtual shield in front of their customers sites, with Layer 3 attacks none of the attack traffic reaches the customer's servers. Traffic to Spamhaus's network dropped to below the levels when the attack started as soon as they signed up for this service.

Source: [https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/]

7. (10 points) Study the Amazon Route 53 service and answer the following questions
a. What does Route 53 do?
b. Why is it called Route 53?
c. What other Amazon services is it designed to work with (please explain how it happens

with one or two examples)?
d. What is the difference between the domain name and hosted zone?
e. Does Route 53 have a default for the Time-to-live (TTL) value?
f. What is the pricing of the service?

Solution:
Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

a.

i. Amazon Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS.
ii. You can use Amazon Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of your application and its endpoints.
iii. Amazon Route 53 Traffic Flow makes it easy for you to manage traffic globally through a variety of routing types, including Latency Based Routing, Geo DNS, Geoproximity, and Weighted Round Robin—all of which can be combined with DNS Failover in order to enable a variety of low-latency, fault-tolerant architectures.
iv. Using Amazon Route 53 Traffic Flow's simple visual editor, you can easily manage how your end-users are routed to your application's endpoints—whether in a single AWS region or distributed around the globe. Amazon Route 53 also offers Domain Name Registration – you can purchase and manage domain names such as example.com and Amazon Route 53 will automatically configure DNS settings for your domains.

b.
The name Route 53 is a reference to TCP or UDP port 53, where DNS server requests are addressed.

c.

i. Amazon Route 53 provides highly available and scalable Domain Name System (DNS), domain name registration, and health-checking web services.
ii. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names like example.com into the numeric IP addresses, such as 192.0.2.1, that computers use to connect to each other.
iii. You can combine your DNS with health-checking services to route traffic to healthy endpoints or to independently monitor and/or alarm on endpoints.
iv. You can also purchase and manage domain names such as example.com and automatically configure DNS settings for your domains. Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS.

d.

i. Domain names (DNS concept) are easily recognizable names for numerically addressed Internet resources. For example, amazon.com is a domain.

ii. A hosted zone (Amazon Route 53 concept) is analogous to a traditional DNS zone file; it represents a collection of records that can be managed together, belonging to a single parent domain name. All resource record sets within a hosted zone must have the hosted zone's domain name as a suffix. For example, the amazon.com hosted zone may contain records named www.amazon.com, and www.aws.amazon.com, but not a record named www.amazon.ca.

e.

i. The time for which a DNS resolver caches a response is set by a value called the time to live (TTL) associated with every record.

ii. Amazon Route 53 **does not** have a default TTL for any record type. You must always specify a TTL for each record so that caching DNS resolvers can cache your DNS records to the length of time specified through the TTL.

f.

With Amazon Route 53, you don't have to pay any upfront fees or commit to the number of queries the service answers for your domain. Like with other AWS services, you pay as you go and only for what you use:

i. Managing hosted zones: You pay a monthly charge for each hosted zone managed with Route 53.
   - Hosted Zones and Records:
     $0.50 per hosted zone / month for the first 25 hosted zones
     $0.10 per hosted zone / month for additional hosted zones

ii. Serving DNS queries: You incur charges for every DNS query answered by the Amazon Route 53 service, except for queries to Alias A records that are mapped to Elastic Load Balancing instances, CloudFront distributions, AWS Elastic Beanstalk environments, API Gateways, VPC endpoints, or Amazon S3 website buckets, which are provided at no additional charge.
   - Queries
     The following query prices are prorated; for example, a hosted zone with 100,000 standard queries / month would be charged $0.04 and a hosted zone with 100,000 Latency-Based Routing queries / month would be charged $0.06.
     I. Standard Queries
        $0.40 per million queries – first 1 Billion queries / month
        $0.20 per million queries – over 1 Billion queries / month
     II. Latency Based Routing Queries
        $0.60 per million queries – first 1 Billion queries / month
        $0.30 per million queries – over 1 Billion queries / month
     III. Geo DNS and Geoproximity Queries
        $0.70 per million queries – first 1 Billion queries / month
        $0.35 per million queries – over 1 Billion queries / month

IV. Alias Queries: Queries to Alias records are provided at no additional cost to current Route 53 customers when the records are mapped to the following AWS resource types:
Elastic Load Balancers
Amazon CloudFront distributions
AWS Elastic Beanstalk environments
Amazon S3 buckets that are configured as website endpoints

iii. Managing domain names: You pay an annual charge for each domain name registered via or transferred into Route 53. Your monthly bill from AWS will list your total usage and dollar amount for the Amazon Route 53 service separately from other AWS services. Pricing for domain names varies by TLD.

Source: [https://en.wikipedia.org/wiki/Amazon_Route_53] [https://aws.amazon.com/route53/] [https://aws.amazon.com/route53/pricing/] [https://aws.amazon.com/route53/faqs/]

8. (10 points) Take a look at https://www.twistlock.com/2018/11/13/open-source-clouddiscovery-tool/ and learn what the Cloud Discovery service is. Explain how the tool works. What does it do? (Just research your answer and explain how you understand it.) Incidentally, this is the tool Amazon uses. Does Route 53 provide a similar service? If so, how? What are the differences?

Solution:

- Cloud Discovery is an open source tool that helps infrastructure, operations, and security teams identify all the cloud native platform services, such as container registries, managed Kubernetes platforms, and serverless services used across your cloud providers, accounts, and regions.
- Cloud Discovery is a powerful tool for audit and security practitioners that want a simple way to discover all the ‘unknown unknowns’ across environments without having to manually login to multiple provider consoles, click through many pages, and manually export the data.

How Cloud Discovery works:

- Cloud Discovery connects to cloud providers’ native platform APIs to discover services and their metadata and requires only read permissions.
- Cloud Discovery also has a network discovery option that uses port scanning to sweep IP ranges and discover cloud native infrastructure and apps, such as Docker Registries and Kubernetes API servers, with weak settings or authentication. This capability is useful for discovering ‘self-installed’ cloud native components not provided as a service by a cloud provider, such as a Docker Registry running on an EC2 instance.
- Cloud Discovery is provided as a simple Docker container image that can be run anywhere and works well for both interactive use and automation.

- Today, Cloud Discovery supports asset identification on AWS, Azure, and Google Cloud Platform but it's designed to be easily pluggable with support for more cloud platforms coming soon.

Service similar to Cloud Discovery provided by Amazon 53:

- AWS Cloud Map is a cloud resource discovery service. With Cloud Map, you can define custom names for your application resources, and it maintains the updated location of these dynamically changing resources. This increases your application availability because your web service always discovers the most up-to-date locations of its resources.
- AWS Cloud Map enables you to map your cloud. You can define friendly names for any resource, such as Amazon S3 buckets, Amazon DynamoDB tables, Amazon SQS queues, or custom cloud services built on Amazon EC2, Amazon ECS, Amazon EKS, or AWS Lambda. Your applications can then discover resource location and metadata by friendly name using the AWS SDK and authenticated API queries. Resources can be further filtered and discovered by custom attributes such as deployment stage or version.
- You can use the Amazon Route 53 Auto Naming API to automate the registration of microservices in DNS. The new API simplifies the management of DNS names and health checks for microservices that run on top of AWS when microservices scale up and down.
- Differences: Amazon Route 53 Auto Naming, which was released on December 05, 2017, automates service name management in DNS and supported IP-based resources only. Cloud Discovery extends the capabilities of the Auto Naming APIs by providing infrastructure, operations, and security teams identify all the cloud native platform services, such as container registries, managed Kubernetes platforms, and serverless services used across your cloud providers, accounts, and regions.

Source: [https://www.twistlock.com/2018/11/13/open-source-cloud-discovery-tool/]
[https://aws.amazon.com/cloud-map/faqs/]