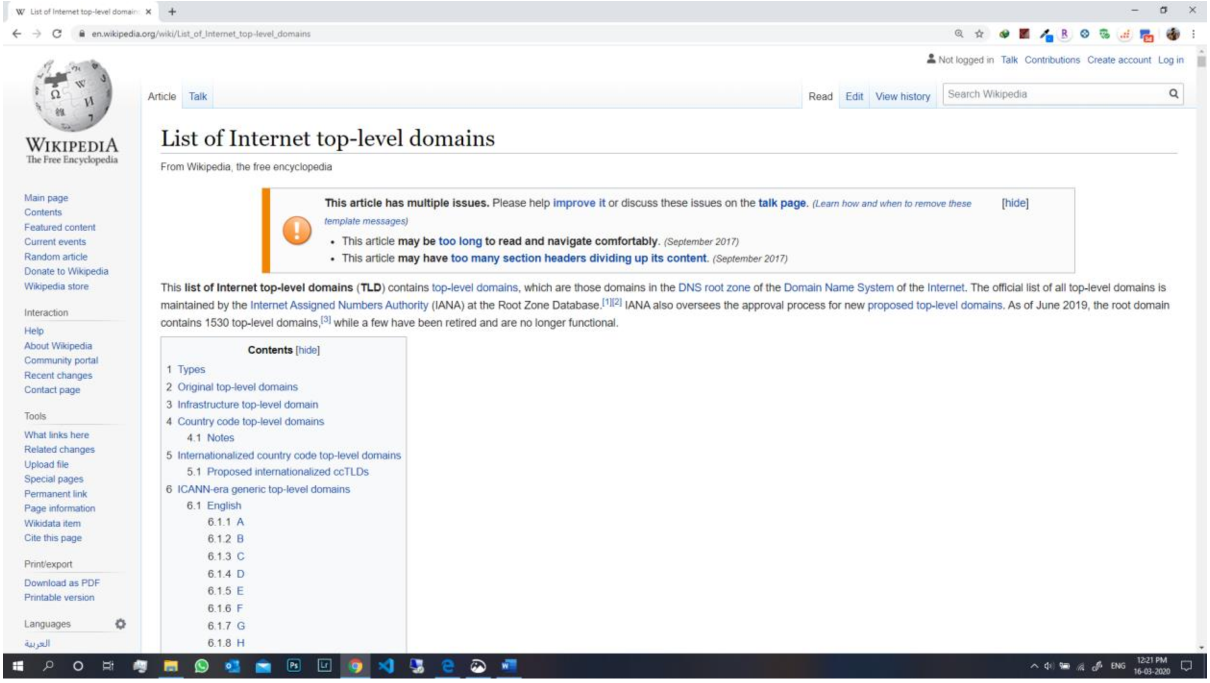
1. (5 points) Find out the exact number of all top domain names. Make sure you put a date and time of your finding. (Hint: use the information given at the lecture to locate the list of names at IANA.)

Ans: Currently, there are **1530** top-level domains. This was my finding on the 16th of March 2020 at 12:21 PM.



List of Internet top-level domains

From Wikipedia, the free encyclopedia

This article has multiple issues. Please help **improve it** or discuss these issues on the **talk page**. *(Learn how and when to remove these template messages)* [hide]

- This article **may be too long to read and navigate comfortably**. *(September 2017)*
- This article **may have too many section headers dividing up its content**. *(September 2017)*

This **list of Internet top-level domains** (**TLD**) contains top-level domains, which are those domains in the DNS root zone of the Domain Name System of the Internet. The official list of all top-level domains is maintained by the Internet Assigned Numbers Authority (IANA) at the Root Zone Database.[1][2] IANA also oversees the approval process for new proposed top-level domains. As of June 2019, the root domain contains 1530 top-level domains,[3] while a few have been retired and are no longer functional.

Contents [hide]

1 Types
2 Original top-level domains
3 Infrastructure top-level domain
4 Country code top-level domains
  4.1 Notes
5 Internationalized country code top-level domains
  5.1 Proposed internationalized ccTLDs
6 ICANN-era generic top-level domains
  6.1 English
    6.1.1 A
    6.1.2 B
    6.1.3 C
    6.1.4 D
    6.1.5 E
    6.1.6 F
    6.1.7 G
    6.1.8 H

(Reference: https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains)

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

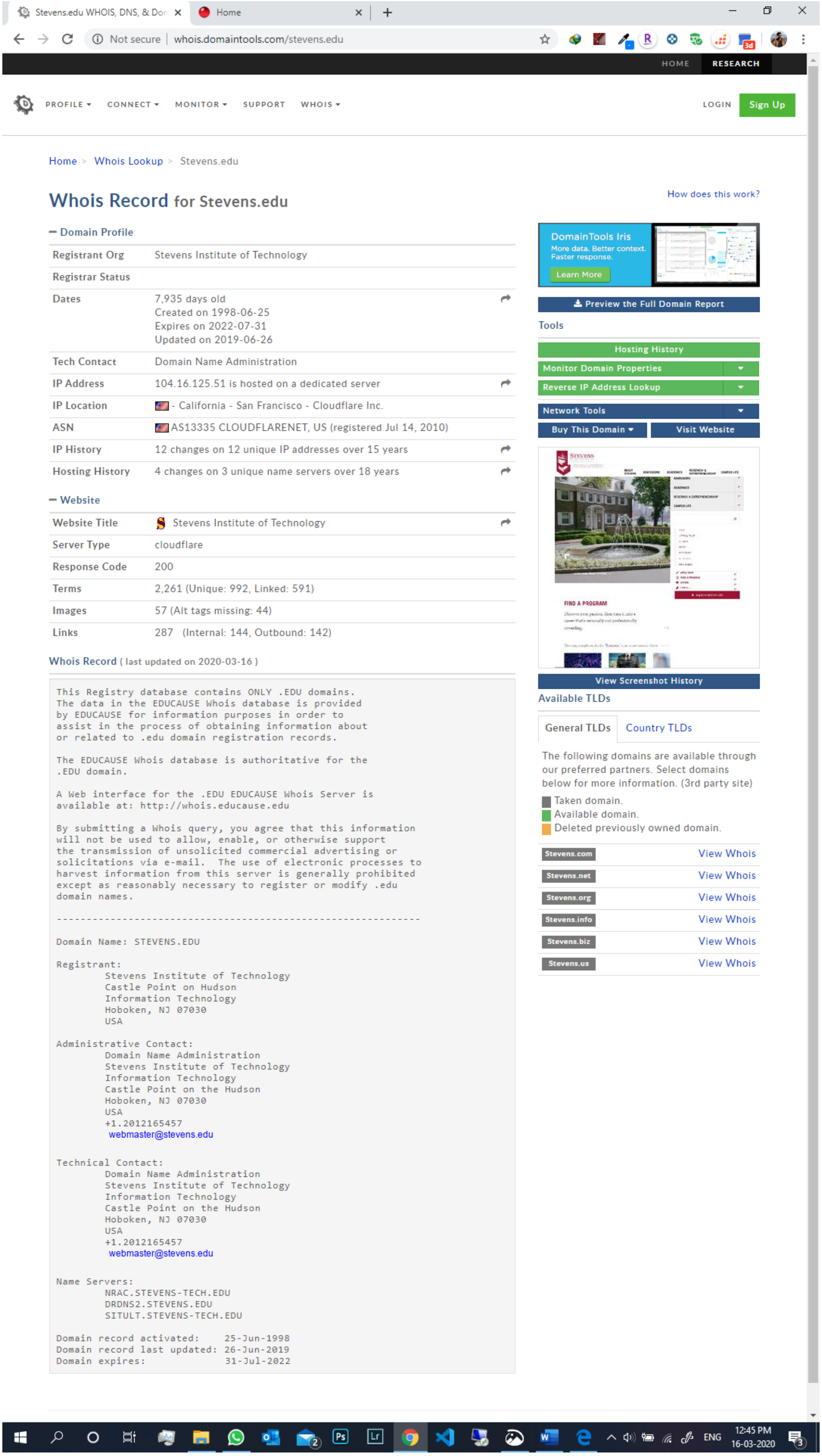
a. Find the information about the stevens.edu domain as well as the domain of some other school (for instance, the school you had studied at before you came to Stevens). Who are the administrative contacts for the domains listed there?

b. Now, what happens when you try to find the administrative contact for the .xxx domain? Explain what you have found.

Ans a: Whois Record for stevens.edu

Administrative Contact:
Domain Name Administration
Stevens Institute of Technology
Information Technology
Castle Point on the Hudson
Hoboken, NJ 07030
USA

+1.2012165457 webmaster@stevens.edu



Stevens.edu WHOIS, DNS, & Dor
Home
Not secure | whois.domaintools.com/stevens.edu
HOME
RESEARCH
PROFILE ▾
CONNECT ▾
MONITOR ▾
SUPPORT
WHOIS ▾
LOGIN
Sign Up

Home > Whois Lookup > Stevens.edu

How does this work?

Whois Record for Stevens.edu

− Domain Profile

Registrant Org	Stevens Institute of Technology
Registrar Status	
Dates	7,935 days old Created on 1998-06-25 Expires on 2022-07-31 Updated on 2019-06-26
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

− Website

Website Title	Stevens Institute of Technology
Server Type	cloudflare
Response Code	200
Terms	2,261 (Unique: 992, Linked: 591)
Images	57 (Alt tags missing: 44)
Links	287 (Internal: 144, Outbound: 142)

Whois Record (last updated on 2020-03-16)

```
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------

Domain Name: STEVENS.EDU

Registrant:
        Stevens Institute of Technology
        Castle Point on Hudson
        Information Technology
        Hoboken, NJ 07030
        USA

Administrative Contact:
        Domain Name Administration
        Stevens Institute of Technology
        Information Technology
        Castle Point on the Hudson
        Hoboken, NJ 07030
        USA
        +1.2012165457
        webmaster@stevens.edu

Technical Contact:
        Domain Name Administration
        Stevens Institute of Technology
        Information Technology
        Castle Point on the Hudson
        Hoboken, NJ 07030
        USA
        +1.2012165457
        webmaster@stevens.edu

Name Servers:
        NRAC.STEVENS-TECH.EDU
        DRDNS2.STEVENS.EDU
        SITULT.STEVENS-TECH.EDU

Domain record activated:    25-Jun-1998
Domain record last updated: 26-Jun-2019
Domain expires:             31-Jul-2022
```

DomainTools Iris
More data. Better context. Faster response.
Learn More
Preview the Full Domain Report

Tools

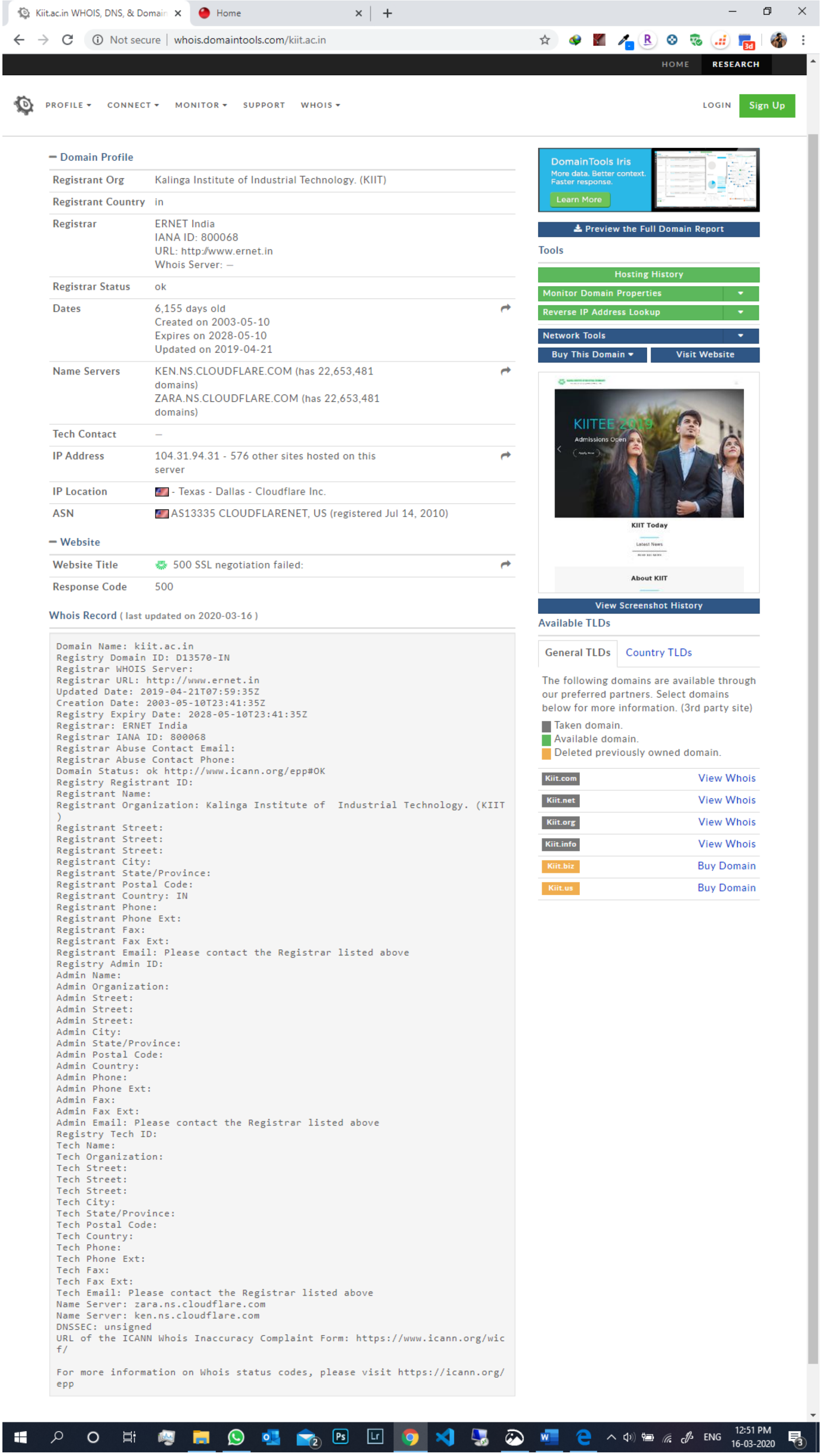
Available TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▨ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

Stevens.com	View Whois
Stevens.net	View Whois
Stevens.org	View Whois
Stevens.info	View Whois
Stevens.biz	View Whois
Stevens.us	View Whois

Whois record for Kiit.ac.in



Domain Profile

Registrant Org	Kalinga Institute of Industrial Technology. (KIIT)
Registrant Country	in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: –
Registrar Status	ok
Dates	6,155 days old Created on 2003-05-10 Expires on 2028-05-10 Updated on 2019-04-21
Name Servers	KEN.NS.CLOUDFLARE.COM (has 22,653,481 domains) ZARA.NS.CLOUDFLARE.COM (has 22,653,481 domains)
Tech Contact	–
IP Address	104.31.94.31 - 576 other sites hosted on this server
IP Location	- Texas - Dallas - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)

Website

Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2020-03-16)

```
Domain Name: kiit.ac.in
Registry Domain ID: D13570-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2019-04-21T07:59:35Z
Creation Date: 2003-05-10T23:41:35Z
Registry Expiry Date: 2028-05-10T23:41:35Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name:
Registrant Organization: Kalinga Institute of  Industrial Technology. (KIIT
)
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech Street:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Please contact the Registrar listed above
Name Server: zara.ns.cloudflare.com
Name Server: ken.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wic
f/

For more information on Whois status codes, please visit https://icann.org/
epp
```

Available TLDs

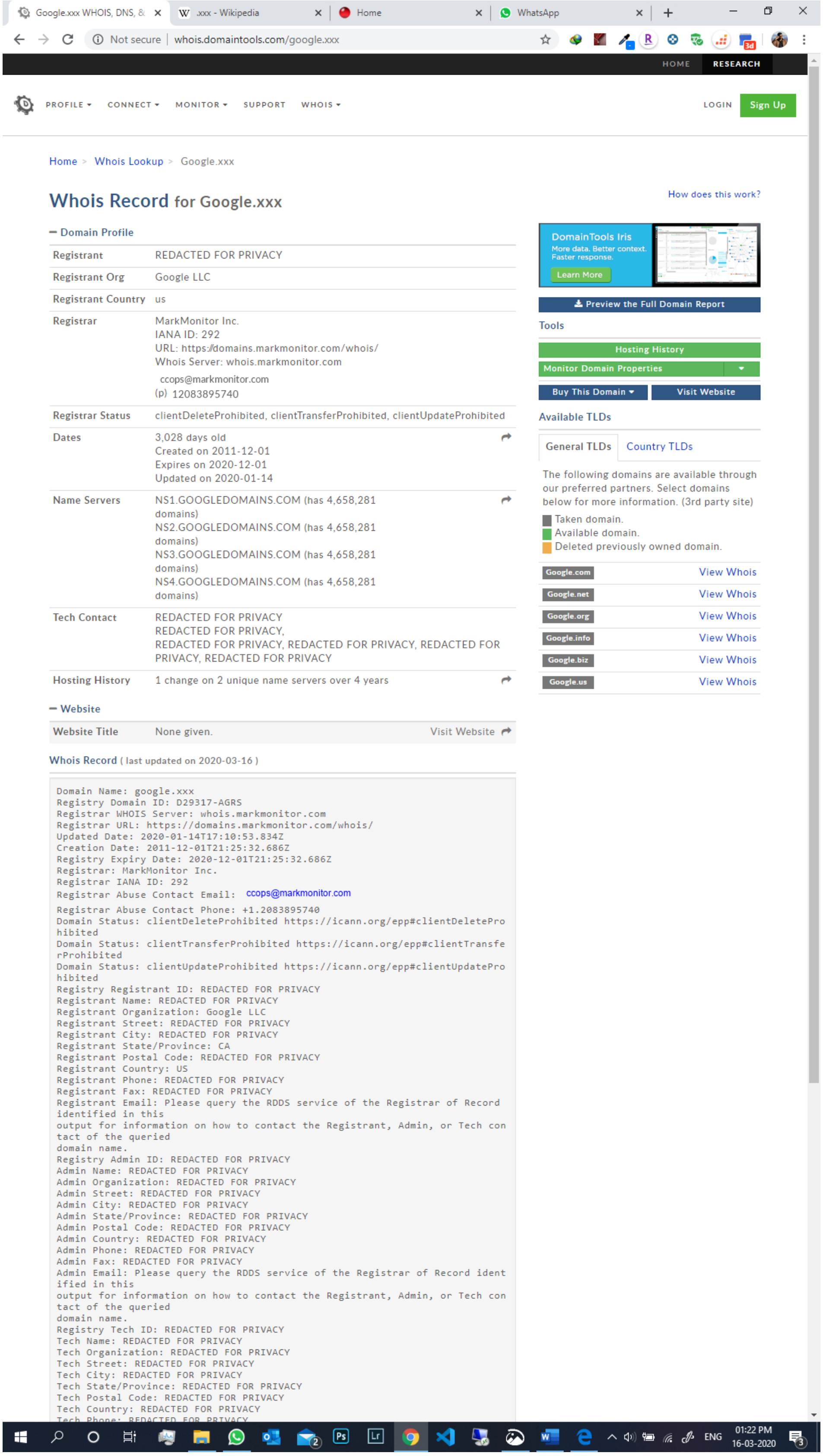
General TLDs | Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

- ■ Taken domain.
- 🟩 Available domain.
- 🟧 Deleted previously owned domain.

Kiit.com	View Whois
Kiit.net	View Whois
Kiit.org	View Whois
Kiit.info	View Whois
Kiit.biz	Buy Domain
Kiit.us	Buy Domain

b. .xxx is a sponsored top-level domain (sTLD) intended as a voluntary option for pornographic sites on the Internet. The sponsoring organization is the International Foundation for Online Responsibility (IFFOR). The registry is operated by ICM Registry LLC. The ICANN Board voted to approve the sTLD on 18 March 2011. It went into operation on 15 April 2011.



Home > Whois Lookup > Google.xxx

Whois Record for Google.xxx

How does this work?

− Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	Google LLC
Registrant Country	us
Registrar	MarkMonitor Inc. IANA ID: 292 URL: https://domains.markmonitor.com/whois/ Whois Server: whois.markmonitor.com ccops@markmonitor.com (p) 12083895740
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	3,028 days old Created on 2011-12-01 Expires on 2020-12-01 Updated on 2020-01-14
Name Servers	NS1.GOOGLEDOMAINS.COM (has 4,658,281 domains) NS2.GOOGLEDOMAINS.COM (has 4,658,281 domains) NS3.GOOGLEDOMAINS.COM (has 4,658,281 domains) NS4.GOOGLEDOMAINS.COM (has 4,658,281 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
Hosting History	1 change on 2 unique name servers over 4 years

− Website

Website Title	None given.	Visit Website

Whois Record (last updated on 2020-03-16)

```
Domain Name: google.xxx
Registry Domain ID: D29317-AGRS
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: https://domains.markmonitor.com/whois/
Updated Date: 2020-01-14T17:10:53.834Z
Creation Date: 2011-12-01T21:25:32.686Z
Registry Expiry Date: 2020-12-01T21:25:32.686Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:  ccops@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeletePro
hibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransfe
rProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePro
hibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Google LLC
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: CA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record
identified in this
output for information on how to contact the Registrant, Admin, or Tech con
tact of the queried
domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record ident
ified in this
output for information on how to contact the Registrant, Admin, or Tech con
tact of the queried
domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
```

Tools

Available TLDs

General TLDs | Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

▇ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

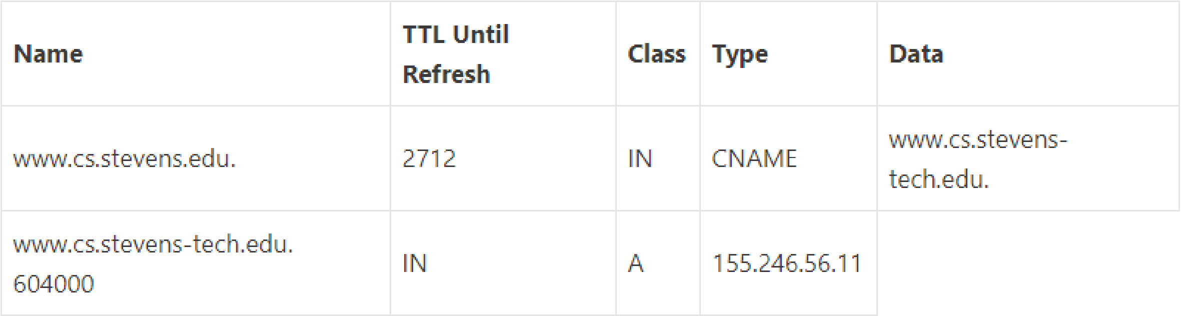
Google.com	View Whois
Google.net	View Whois
Google.org	View Whois
Google.info	View Whois
Google.biz	View Whois
Google.us	View Whois

3. (5 points) Lookup 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!)

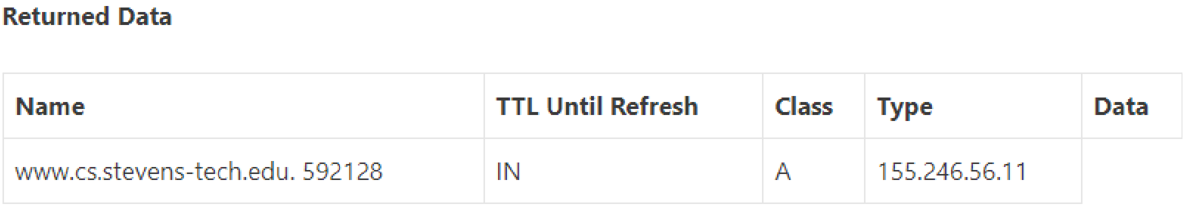
Does Stevens specify IPV6 addresses to any of its hosts? Does Google?

Ans:



Name	TTL Until Refresh	Class	Type	Data
www.cs.stevens.edu.	2712	IN	CNAME	www.cs.stevens-tech.edu.
www.cs.stevens-tech.edu. 604000	IN	A	155.246.56.11	

After entering the returned cname as the host, we get the following:



Returned Data

Name	TTL Until Refresh	Class	Type	Data
www.cs.stevens-tech.edu. 592128	IN	A	155.246.56.11	

- **A:** the IPv4 address of the domain.
- **AAAA:** the domain’s IPv6 address.
- **CNAME:** the canonical name — allowing one domain name to map on to another. This allows more than one website to refer to a single web server.
- **MX:** the server that handles email for the domain.
- **NS:** one or more authoritative name server records for the domain.
- **TXT:** a record containing information for use outside the DNS server. The content takes the form of name=value. This information is used for many things including authentication schemes such as SPF and DKIM.
- **TTL:** Time to Live

After reverse DNS lookup (https://dnsquery.org/ip2location/www.cs.stevens-tech.edu), the following data was found:

Country: United States (US)

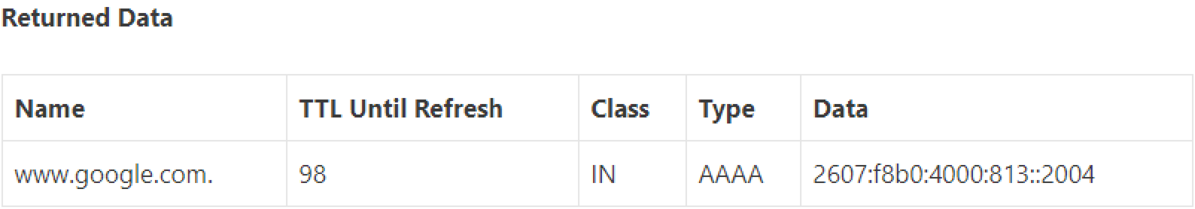
City: Hoboken

Latitude: 40.7458

Longitude: -74.0321

No, Stevens does not share its IPv6 address since the AAAA query returned NULL.

Yes, Google does share its IPv6 address. Below is a screenshot of the result retrieved from the AAAA query.



Returned Data

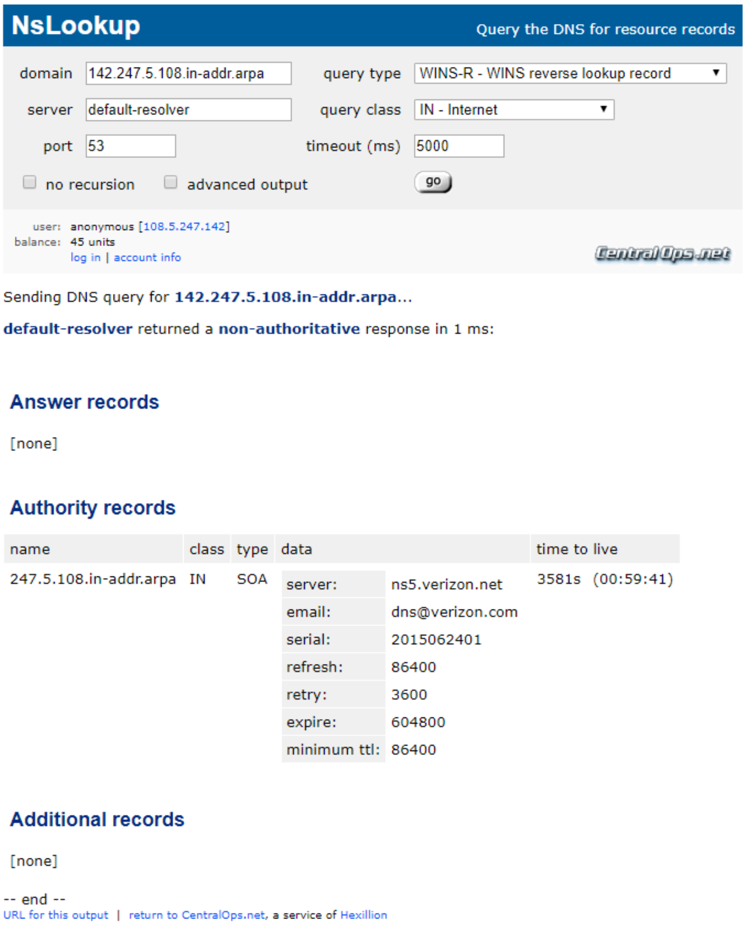
Name	TTL Until Refresh	Class	Type	Data
www.google.com.	98	IN	AAAA	2607:f8b0:4000:813::2004

This information was recorded on the 16th of March at 4:57 PM.

(Reference: https://network-tools.com/nslookup/ , https://centralops.net/co/NsLookup.aspx , http://www.kloth.net/services/nslookup.php & https://dnsquery.org/)

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 lookup? If you can, what is the domain name? If you cannot, explain why.

Ans: Yes, I can find my domain with the reverse lookup. Below are all the details of the reverse lookup query:



NsLookup Query the DNS for resource records

domain: 142.247.5.108.in-addr.arpa
query type: WINS-R - WINS reverse lookup record
server: default-resolver
query class: IN - Internet
port: 53
timeout (ms): 5000
□ no recursion □ advanced output

user: anonymous [108.5.247.142]
balance: 45 units
log in | account info

Sending DNS query for **142.247.5.108.in-addr.arpa**...

default-resolver returned a **non-authoritative** response in 1 ms:

Answer records

[none]

Authority records

name	class	type	data		time to live
247.5.108.in-addr.arpa	IN	SOA	server:	ns5.verizon.net	3581s (00:59:41)
			email:	dns@verizon.com	
			serial:	2015062401	
			refresh:	86400	
			retry:	3600	
			expire:	604800	
			minimum ttl:	86400	

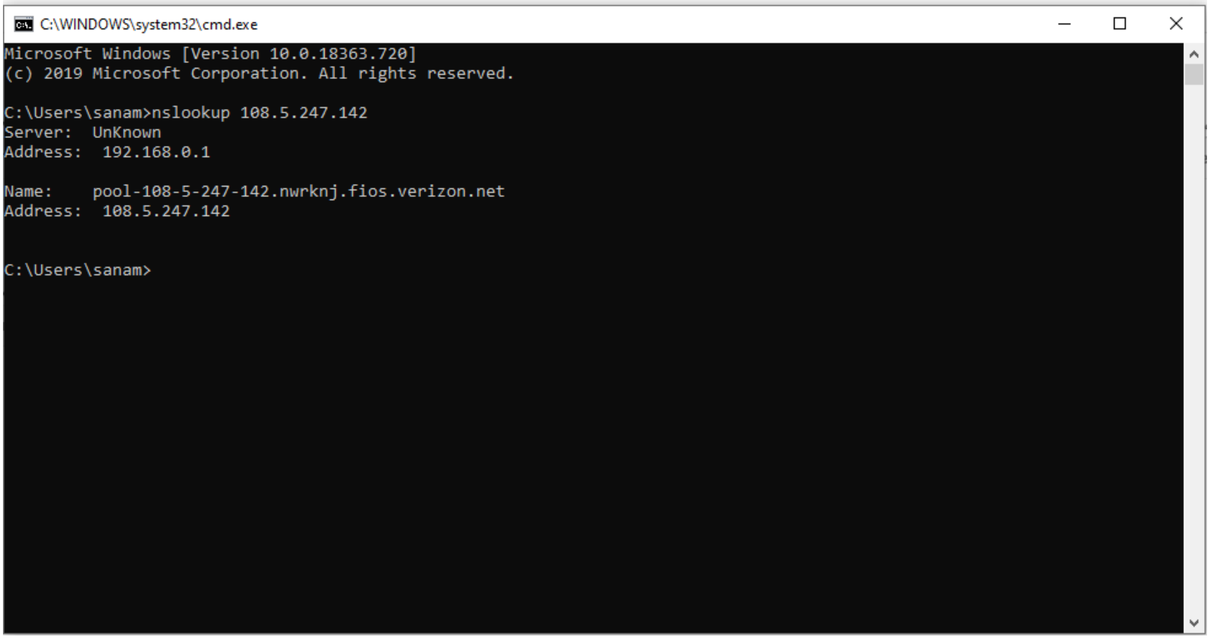
Additional records

[none]

-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

I found my IP address by searching What's my IP in google.



```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\sanam>nslookup 108.5.247.142
Server:  UnKnown
Address:  192.168.0.1

Name:    pool-108-5-247-142.nwrknj.fios.verizon.net
Address:  108.5.247.142


C:\Users\sanam>
```

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?

Ans:

Structure and Responsibilities of IANA

The **Internet Assigned Numbers Authority (IANA)** is a department of ICANN, a non-profit private American corporation. IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. Their various activities can be broadly grouped into three categories:

- **Domain Names:** Management of the DNS Root, the .int and .arpa domains, and an IDN practices resources.
- **Number Resources:** Co-ordination of the global pool of IP and AS numbers, primarily providing them to Regional Internet Registries.
- **Protocol Assignments:** Internet protocols' numbering systems are managed in conjunction with standards bodies.

Structure and Responsibilities of ICANN

ICANN is made up of several different groups, each of which represents a different interest on the internet and all of which contribute to any final decisions that ICANN's make. Three supporting organizations deal with IP addresses, domain names, and manage of country code top-level domains. Four advisory committees provide advice and recommendations. And finally, there is a Technical Liason Group which works with organizations that devise the basic protocols for internet technologies. The roles of ICANN are:

- It includes the consideration and implementation of new TLDs and the introduction of IDNS'.

- It coordinates the global Internet's system of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems.
- It formalizes relationships with root name server operators.
- It ensures appropriate contingency planning, maintains clear processes in root zone changes.
- It maintains and improves the multi-stakeholder model and the global participation of all stakeholders, and will continue to further the effectiveness of the bottom-up policy development processes.
- It implements appropriate mechanisms that foster participation in ICANN by global Internet stakeholders, such as providing educational services and fostering information sharing for constituents and promoting best practices among industry segments.
- It shall conduct a review of and shall make necessary changes in, corporate administrative structure to ensure stability, including devoting adequate resources to contract enforcement, taking into account organizational and corporate governance best practices.

Differences in responsibilities between IANA and ICANN

- IANA is the institution that runs TLDS whereas, ICANN based on the Memorandum of Understanding (MoU), is the institution that runs IANA.
- IANA runs Top-Level Domains and manages the task of IP address and ranges, ports, and other related characteristics whereas, ICANN is a non-profit association that coordinates the Internet's worldwide space framework.

Controversy in ICANN concerning Whois

Internet regulators are pushing a controversial plan to restrict public access to WHOIS Web site registration records. Proponents of the proposal say it would improve the accuracy of WHOIS data and better protect the privacy of people who register domain names. Critics argue that such a shift would be unworkable and make it more difficult to combat phishers, spammers and scammers. A working group within The Internet Corporation for Assigned Names and Numbers (ICANN), the organization that oversees the Internet's domain name system, has proposed scrapping the current WHOIS system — which is inconsistently managed by hundreds of domain registrars and allows anyone to query Web site registration records. To replace the current system, the group proposes creating a more centralized WHOIS lookup system that is closed by default. According to an interim report (PDF) by the ICANN working group, the WHOIS data would be accessible only to "authenticated requestors that are held accountable for appropriate use" of the information.

(Reference: https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority , https://www.iana.org, https://www.icann.org/resources/pages/what-2012-02-25-en & http://www.securityweek.com/icanns-rolling-controversyverification-whois-registration-data)

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.

Ans a:

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 can both amplify the magnitude of the traffic directed against a DDOS victim and conceal the source of the attacking machines.

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 co-opted by attackers and used in criminal attacks on third parties.

In 2008 ISC CTO Joao Damas co-authored RFC 5358,
"Preventing Use of Recursive Nameservers in Reflector Attacks." For 8 years now we've been consistently leading on this issue as part of our mission to strengthen the DNS infrastructure, improve network security, and contribute to stable and open internet.

1. Spamhaus is coming from a technique that has been known for years — a variety of reflection attacks commonly known as a “DNS amplification attack. As an industry leader in the field of DNS software, ISC sees the Spamhaus DDOS as a perfect opportunity to remind DNS operators why it is important to not operate an “open” recursive resolver, a policy recommendation we have been making since 2005.

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 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 co-opted by attackers and used in criminal attacks on third parties.

2. 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. Spamhaus's blocklists are distributed via DNS and there is a long list of volunteer organizations that mirror their DNS infrastructure to ensure it is resilient to attacks. The website, however, was unreachable.

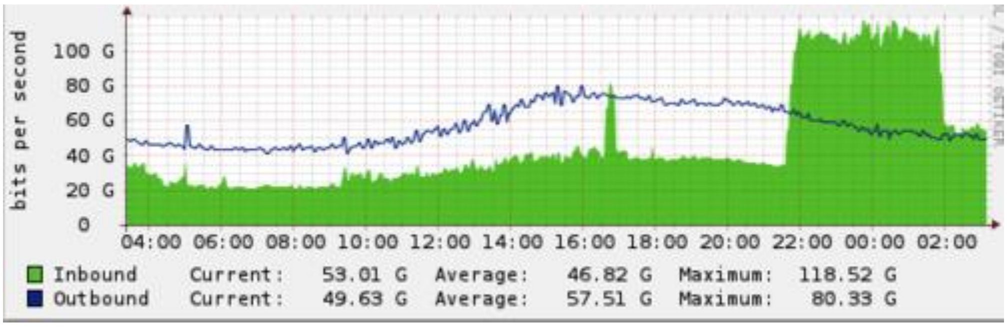
Very large Layer 3 attacks are nearly always originated from many sources. These many sources each send traffic to a single Internet location, effectively creating a tidal wave that overwhelms the target's resources. In this sense, the attack is distributed (the first D in DDoS -- Distributed Denial of Service). The sources of attack traffic can be a group of individuals working together (e.g., the Anonymous LOIC model, although this is Layer 7 traffic and even at high volumes usually much smaller in volume than other methods), a botnet of compromised PCs, a botnet of compromised servers, misconfigured DNS resolvers, or even home Internet routers with weak passwords.

Since an attacker attempting to launch a Layer 3 attack doesn't care about receiving a response to the requests they send, the packets that make up the attack do not have to be accurate or correctly formatted. Attackers will regularly spoof all the information in the attack packets, including the source IP, making it look like the attack is coming from a virtually infinite number of sources. Since packets data can be fully randomized, using techniques like IP filtering even upstream becomes virtually useless.

On March 19, 2013 afternoon, CloudFlare was contacted by the non-profit anti-spam organization Spamhaus. They were suffering a large DDoS attack against their website and asked if we could help mitigate the attack.

Cloudflare immediately mitigated the attack, making the site once again reachable. (More on how we did that below.) Once on our network, we 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 we use for DDoS scrubbing. The green area represents inbound requests and the blue line represents out-bound responses. While there is always some attack traffic on our 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 I'm writing this at 16:15 UTC on March 20, 2013, it appears the attack is picking up again.



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 a 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.

We 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. It is worth repeating: open DNS resolvers are the scourge of the Internet and these attacks will become more common and large until service providers take serious efforts to close them.

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. Cloudflare made heavy use of Anycast. That means the same IP address is announced from every one of our 23 worldwide data centers. The network itself load balances requests to the nearest facility. Under normal circumstances, this helps us ensure a visitor is routed to the nearest data center on our network.

When there's an attack, Anycast serves to effectively dilute it by spreading it across our 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 our data centers. Because Cloudflare acts as a virtual shield in front of our customer's 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 our service. While the majority of the traffic involved in the attack was DNS reflection, the attacker threw in a few other attack methods as well. One was a so-called ACK reflection attack. When a TCP connection is established there is a handshake. The server initiating the TCP session first sends a SYN (for synchronize) request to the receiving server. The receiving server responds with an ACK (for acknowledge). After that handshake, data can be exchanged.

In an ACK reflection, the attacker sends many SYN packets to servers with a spoofed source IP address pointing to the intended victim. The servers then respond to the victim's IP with an ACK. Like the DNS reflection

attack, this disguises the source of the attack, making it appear to come from legitimate servers. However, unlike the DNS reflection attack, there is no amplification factor: the bandwidth from the ACKs is symmetrical to the bandwidth the attacker has to generate the SYNs. Cloudflare is configured to drop unmatched ACKs, which mitigates these types of attacks.

Whenever Cloudflare sees one of these large attacks, network operators will write to us upset that we are attacking their infrastructure with abusive DNS queries or SYN floods. It is their infrastructure that is being used to reflect an attack at us. By working with and educating network operators, they clean up their network which helps to solve the root cause of these large attacks.

(Reference: 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?

Ans:

a: 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. Amazon Route 53 is fully compliant with IPv6 as well.

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. 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. 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 to enable a variety of low-latency, fault-tolerant architectures. 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: It has been named as Route 53 since it refers to TCP or UDP port 53 and handles all DNS requests through port 53.

c: Amazon Route 53 is designed to work well with other AWS features and offerings. You can use Amazon Route 53 to map domain names to your Amazon EC2 instances, Amazon S3 buckets, Amazon CloudFront distributions, and other AWS resources. By using the AWS Identity and Access Management (IAM) service with Amazon Route 53, you get fine-grained control over who can update your DNS data. You can use Amazon Route 53 to map your zone apex (example.com versus www.example.com) to your Elastic Load Balancing instance, Amazon CloudFront distribution, AWS Elastic Beanstalk environment, or Amazon S3 website bucket using a feature called Alias record.

d: A domain is a general DNS concept. Domain names are easily recognizable names for numerically addressed Internet resources. For example, amazon.com is a domain. A hosted zone is an Amazon Route 53 concept. A hosted zone 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 . You can use the Route 53 Management Console or API to create, inspect, modify, and delete hosted zones. You can also use the Management Console or API to register new domain names and transfer in existing domain names into Route 53's management.

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

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

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.

Standard Queries

- $0.40 per million queries – first 1 Billion queries / month
- $0.20 per million queries – over 1 Billion queries / month

Latency Based Routing Queries

- $0.60 per million queries – first 1 Billion queries / month
- $0.30 per million queries – over 1 Billion queries / month

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

Traffic Flow

$50.00 per policy record / month

You create a policy record when you associate an Amazon Route 53 Traffic Flow policy with a specific DNS name (such as www.example.com) so that the traffic policy manages traffic for that DNS name. The monthly price listed above is prorated for partial months. There is no charge for traffic policies that are not associated with a DNS name via a policy record.

Health Checks

Get Started With DNS Failover At No Additional Cost*
New and existing customers can create up to 50 health checks for AWS endpoints** that are within or linked to the same AWS account.

	AWS Endpoints	**Non-AWS Endpoints**
Basic Health Checks	$0.50* per health check / month	$0.75 per health check / month
Optional health check features: HTTPS; String Matching; Fast Interval; Latency Measurement	$1.00 / month per optional feature	$2.00 / month per optional feature

Route 53 Resolver

Route 53 Resolver endpoints

A Route 53 Resolver endpoint requires two or more IP addresses. Each IP address corresponds with one elastic network interface (ENI). A single outbound endpoint can be used by multiple VPCs that were created by multiple accounts within the same region.

- $0.125 per ENI / hour

Recursive DNS queries to and from on-premises networks

Only queries that pass through a Route 53 resolver endpoint going to or coming from on-premises resources will be charged. Queries that resolve locally to your Virtual Private Cloud (VPC) will not be charged.

- $0.40 per million queries - first 1 Billion queries / month
- $0.20 per million queries - over 1 Billion queries / month

(Reference: https://aws.amazon.com/route53/pricing/ , https://aws.amazon.com/route53/ , https://aws.amazon.com/route53/faqs/ & https://en.wikipedia.org/wiki/Amazon_Route_53)

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?

Ans: Cloud discovery is an open-source tool that helps infrastructure, operations and security teams identify all the cloud-native platform services such as serverless services, managed Kubernetes platforms used across cloud providers.

Cloud discovery connects to the cloud provider's native platform APIs to discover services and their metadata and requires only read permissions. It has network discovery options that use port scanning to sweep IP ranges and discover cloud-native infrastructure and apps such as Docker registries and Kubernetes API servers.

Cloud discovery is provided as a simple Docker container image that will work everywhere for automation and interactive use.

Amazon Route 53 Auto Naming, which was released on December 05, 2017, automates service name management in DNS and supported IP-based resources only. AWS Cloud Map extends the capabilities of the Auto Naming APIs by providing a service registry for resources, represented by IPs, URLs, and ARNs and offering an API-based service discovery mechanism with a faster change propagation and the ability to use attributes to narrow down the set of discovered resources. All the existing Amazon Route 53 Auto Naming resources are automatically upgraded to AWS Cloud Map and are available for API-based discovery.

(Reference: https://docs.aws.amazon.com/cloud-map/latest/dg/what-is-cloud-map.html)