HW-4

1) The exact number of the top-level domains(TLDs), which are highest level in hierarchial domain name system(DNS) after the root, were a total of **1589** in **March 2021**. I found this answer on 4/3/2022 on 10:45PM EST. The official list of all the top-level domains is maintained by the Internet Assigned Numbers Authority (IANA).

*Source: Wikipedia: List of Internet Top-level domain names (*[*https://en.wikipedia.org/wiki/List\_of\_Internet\_top-level\_domains*](https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains) *)*

2)

i) After searching stevens.edu on http://whois.domaintools.com ,the contact information is as follows:

Administrative Contact:

Domain Name Administration

Stevens Institute of Technology

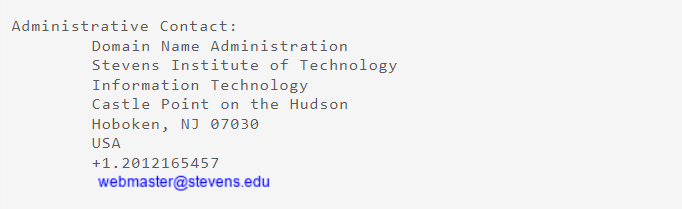
Information Technology

Castle Point on the Hudson

Hoboken, NJ 07030

USA

+1.2012165457



Now, we search the domain for my previous college - Dayananda Sagar college of Engineering(DSCE) - *dsce.edu.in* . The administrative details for this domain are not visible and displayed as "REDACTED FOR PRIVACY", as depicted below:

Admin Name: REDACTED FOR PRIVACY

Admin Organization: REDACTED FOR PRIVACY

Admin Street: REDACTED FOR PRIVACY

Admin Street: 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 Phone Ext: REDACTED FOR PRIVACY

Admin Fax: REDACTED FOR PRIVACY

Admin Fax Ext: REDACTED FOR PRIVACY

Admin Email: Please contact the Registrar listed above

Such message is shown since the information is hidden away because whoever that’s owning the domain didn’t want people to have access to that information. In our case the college has chosen to keep these details private.

ii) Upon searching the .xxx on https://whois.domaintools.com ,we get following administrative details:

Admin Name: Moniker Privacy Services

Admin Organization: Moniker Privacy Services

Admin Street: 2320 NE 9th St, Second Floor

Admin City: Fort Lauderdale

Admin State/Province: FL

Admin Postal Code: 33304

Admin Country: US

Admin Phone: +1.8006886311

Admin Phone Ext:

Admin Fax: +1.9545859186

Admin Fax Ext:

Admin Email:

xxx is a new Sponsored Top-Level Domain (sTLD), specifically designed for the benefit of the global online adult entertainment industry. It will work alongside the other existing ICANN accredited TLDs such as .com, .net, .org, etc. and offers significant benefits and advantages to both providers and consumers.

*Sources: WhoIs Domain Tools(* [*https://whois.domaintools.com*](https://whois.domaintools.com) *), InterNIC(* [*https://www.internic.net/*](https://www.internic.net/) *), Stack overflow(* [*https://stackoverflow.com/questions/54266431/whats-the-meaning-of-redacted-for-privacy*](https://stackoverflow.com/questions/54266431/whats-the-meaning-of-redacted-for-privacy) *)*

3)

**Structure and responsibility of IANA:**

The Internet Assigned Numbers Authority (IANA) is a standards organization 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.

It is a function of Internet Corporation for Assigned Names and Numbers (ICANN). ICANN managed IANA directly from 1998 through 2016, when it was transferred to Public Technical Identifiers (PTI), an affiliate of ICANN that operates IANA today. There three main areas of it responsibilities:-

i) Domain Names: IANA operates and maintains a number of key aspects of the DNS, including the root zone, and the .int and .arpa domains.

ii) Number Resources: management of the worldwide pool of IP and AS numbers, primarily providing them to Regional Internet Registries (RIRs).

iii)Protocol Assignments: IANA is responsible for maintaining many of the codes and numbers contained in a variety of Internet protocols, enumerated below. We provide this service in coordination with the Internet Engineering Task Force (IETF).

**Structure and responsibility of ICANN:**

The Internet Corporation for Assigned Names and Numbers (ICANN) is an American multistakeholder 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.

ICANN consists of many different organizations involved with the internet which have a role in its decision making process. The ICANN currently comprises of three supporting organizations and four advisory committees apart from the Board of Directors and other advisory committees.

The supporting organizations are:-

i)Address Supporting Organization - are tasked with policy making on IP Addresses

ii)Country Code Name Supporting Organization - are tasked with policy making on country code top level domain

iii)Generic Name Supporting Organization - are tasked with policy making on generic top level domain respectively.

The four Advisory Committees are:

i) Governmental Advisory Committee (GAC) - he GAC is composed of representatives from the national governments across the world.

ii)Security and Stability Advisory Committee (SSAC) – The SSAC comprises of cyber security experts tasked to study security issues related to ICANN’s mandate.

iii)Root Server System Advisory Committee (RSSAC) – The RSSAC also comprises of technical experts who provides recommendation and advise on the operation of the DNS root server system.

iv)At-Large Advisory Committee (ALAC) – The ALAC consists of representatives from the organizations of individual internet users. The main function of the ALAC is to "consider and provide advice on the activities of ICANN, in so far as they relate to the interests of individual internet users."

The Board of Directors comprises of 16 members ("Directors") who have voting rights. Additionally it has five non-voting liaisons. There is a Technical Liaison Group which works with organizations that devise the basic protocols for internet technologies.

**The responsibilities of ICANN are:**

i)Coordination of the internet's system of unique identifiers and ensure smooth operation

ii) Consideration and implementation of new TLDs and IDNS.

iii) formalize relationships with root name server operators.

iv) helps maintain processes for root zone changes

v) it promotes the universal participation of all the stakeholders in multiple stakeholder model.

vi) it promotes a bottom-up development model

vii) Gives training services and encourages information sharing among constituents as best practices in the industry.

viii) carries out an overall review of the organization governing structure and make the required modifications to ensure stability, contract enforcement and best practices.

**Differences between IANA and ICANN roles:**

|  |  |  |
| --- | --- | --- |
|  | **IANA** | **ICANN** |
| 1 | IANA is the institution which runs Top Level Domains (TLDs) | ICANN is the institution that run IANA and based on memorandum of understanding |
| 2 | IANA manages task of IP address, ranges, ports, and other related features and runs top-level Domains | ICANN is a non-profit association that coordinate Internet’s worldwide space framework |

**ICANN Whois controversy:**

There is an attempt by the internet agencies to restrict access to WhoIs registration record from general public users in order to increase data security and privacy for those registering domains. ICANN groups are promoting the replacement of the current system managed by several domain registrars worldwide by a centralized system that is closed as a rule to general users except those that are trusted to use it appropriately. The possible implementation for this is detailed in an interim report published by the concerned group in ICANN working on it.

*Sources: IANA website(* [*https://www.iana.org/*](https://www.iana.org/) *), Wiki(* [*https://en.wikipedia.org/wiki/Internet\_Assigned\_Numbers\_Authority*](https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority) *), ICANN website(* [*https://www.icann.org/*](https://www.icann.org/) *), Security Week on Whois controversy(* [*http://www.securityweek.com/icanns-rolling-controversyverification-whois-registration-data*](http://www.securityweek.com/icanns-rolling-controversyverification-whois-registration-data) *), Wiki(* [*https://en.wikipedia.org/wiki/ICANN*](https://en.wikipedia.org/wiki/ICANN) *)*

4)

i) The Spamhaus attack of 2013 was a distributed denial of service(DDoS) attack that targeted the Spamhaus project – an anti-spam project that tracks and compiles lists of the IPs of spammers. The attack was launched by group/s that disagreed with the project’s decision to include cyberbunker as a spam source. The spamhaus attack was made possible due use of Open recursive resolvers by Spamhaus project despite warnings by Internet Systems Consortium(ISC).

Open recursive resolvers accept recursive queries from all IP addresses and is exposed to the Internet. Spamhaus was attacked by a common technique known as "DNS amplification attack" - which takes advantage of the fact that the answer to a query can be much larger than the query itself - to overwhelm the victim. By using the a forged "spoofed" address for a query to open resolver - which believes it originated the request - the attackers reflect a large traffic to victim that they did not request, amplified to a factor 40.

*Sources: Is Your Open DNS Resolver Part of a Criminal Conspiracy? (* [*https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/*](https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/) *), How Spamhaus’ attackers turned DNS into a weapon of mass destruction(* [*https://arstechnica.com/information-technology/2013/03/how-spamhaus-attackers-turned-dns-into-a-weapon-of-mass-destruction/*](https://arstechnica.com/information-technology/2013/03/how-spamhaus-attackers-turned-dns-into-a-weapon-of-mass-destruction/) *)*

ii)

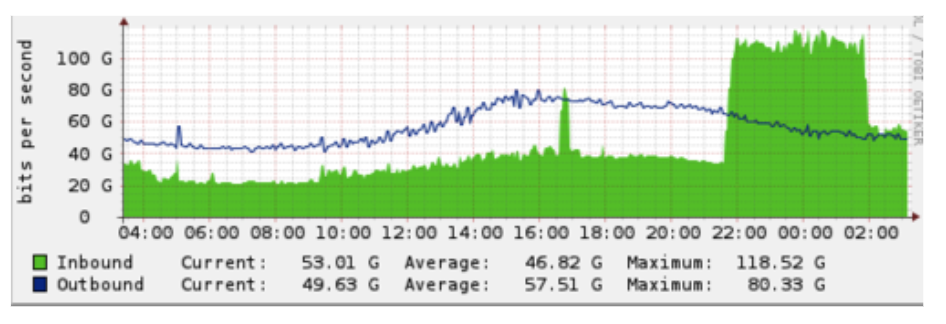
Beginning on March 18, the Spamhaus site came under attack. The attack was large enough that the Spamhaus team wasn’t sure of its size. It was sufficiently large to fully saturate their connection to the rest of the Internet and knock their site offline. These very large attacks, which are known as Layer 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 in order to ensure it is resilient to attacks. The website, however, was unreachable.

Such large scale attacks are generally come from a multiple sources that are spoofed by the malicious group to carry out the attack. These multiple spoofed sources create a distrbuted denial of service(DDOS) attack (distributed here meaning the distributed nature of the attacks origins). THe DDOS attack basically overwhelms the victims resources by exceeding its maximum bandwidth. The source may include multiple individuals working together, a botnet of compromised servers, misconfigured DNS resolvers, a botnet of compromised PCs or even home vulnerable internet routers.

Attackers typically do not bother about the response given they just want to frustrate and deny the target's serviceability. Hence, they spoof all the information in the attck packets including the source IPs to create the impression that the attack originates from virtually infinite legitimate sources. Since packets data can be fully randomized, using techniques like IP filtering even upstream becomes virtually useless.

On March 19th, 2013, Cloudfare was contacted by the anti-spam organization Spamhaus, regarding the DDoS attck they had faced and requested to help mitigate it.

CloudFlare immediately helped to resolve the attack and made the site reachable again after a short duration. This is described below. firstly the cloudfare began recording data about the attack. Initilally the attack was relatively modest at about 10GBPS. There was a brief spike around 16:30 UTC that lasted approximately 10 minutes (probably a test by the attackers). Then, around 21:30 UTC, the attackers let loose a very large magnitude of attack. The graph below is generated from bandwidth samples across a number of the routers that sit in front of servers that we use 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 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.



CloudFare observed that in the Spamhaus case the attackers were requesting the DNS zone file for ripe.net via the DNS open recursive resolvers, and the response was approximately 3000 bytes - a 100-times amplification rate. It detected over 30,000 unique DNS resolvers involved in the attack. This translatesd to each open DNS resolver sending an average of 2.5Mbps, which is small enough avoid detection of most DNS resolvers. Since the attackers used a DNS amplification, they 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 scale DDoS attcks will be difficult to stop for any on-premise system, Cloudfare was designed to deal with these kinds of attacks from the very beginning. It uses Anycast - which gives a the same common IP to each of the 23 data centers aroud the world. The network also automatically load balances itself which in normal times helps to route a requests to their nearest data centers.

This plays a huge role in mitigating the effects of the DDoS attack. This accomplished as follows. Since there are 23 worldwide servers, the traffic automatically gets distributed to all these different locations unburdening any single location. Since the anycast ensures that all the centers have the same IP address this prevents the attackers from being able to target any single location. The attack, in effect, changes from being many-to-one to many-to-many hence significantly reducing its effectiveness.

Once diluted, the attack became relatively much easier to stop at each of the individual data centers. Since the CloudFlare system acts as a virtual shield in front of our customers sites, with Layer 3 attacks none of the attack traffic reaches the customer's servers. The malicious traffic to Spamhaus sites fell to a level below the one recorded before the attack started once they availed the cloudfare service.

While the bulk of the attack was DNS reflection, the attackers threw in some ACK refection attack as well. These attacks involve the use of system ACK(acknowledge) message that follows the SYN(synchromize) messgae as part of the handshakes between two systems looking to estabish a TCP connection. Normally, a system initiating connection, sends a SYN request that is in turn resonded to by the recipient by an ACK message. In the case of Spanhaus attacks, the spoofed sources were used to send SYN request to many systems pointing at the intended victim(here the spamhaus server). These ystems respond to the SYN with an ACK message sent to the victim. This way, similar to DNS reflection, the real identity of the attacking systems is disguised. However, unlike the DNS reflection, no amplification in possible here as the bandwidth from the ACKs is symmetrical to the bandwidth the attacker has to generate the SYNs. Since CloudFlare is configured to drop unmatched ACK messages this type of attack was mitigated.

Whenever CloudFlare see 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. In fact, 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.

*Source: The DDoS That Knocked Spamhaus Offline (And How We Mitigated It) (* [*https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/*](https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/) *)*

5) 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. Amazon Route 53 is fully compliant with IPv6 as well

i) Amazon Route 53 allows you to register new domain name or transfer an existing domain name and supports domain registration for a wide variety of generic-top-level domains (such as .org or .cim) and geographic top level domains (such as .uk or .us). It helps in creation, updating, and management of public DNS records, helps you manage the IP addresses listed for domains names in Internet’s DNS phonebook. Route 53 translates specific domain name like www.example.com in to their corresponding IP address like 192.0.2.1. In addition, it sends automated requests over the Internet to your application to verify that it’s reachable, available, and functional and offers health check to monitor health and performance of your application as well as web servers and other resources.

ii) It is named Route 53 because in lands all TCP or UDP requests on port 53.

iii) Amazon Route 53 can work well with Amazon EC2 instances, Amazon S3 buckets, Amazon CloudFront distributions amongst other AWS resources.

You can also use Identity and Access Management(IAM) service to get fine-grained control over who accesses your DNS settings.

You can use your Route 53 to map your zone apex to your elastic load balancing, Elastic beanstalk, cloudfront distribution or S3 buckets.

iv) A domain is a DNS concept and is easily recognized as such ( for eg., stevens.edu is a domain held by stevens university). A hosted zone is an Amazon Route 53 concept. It is comparable to a traditional DNS zone file and represents a collection of records that can be managed together, belonging to a single parent domain name. Every resource record set within a hosted zone must have the hosted zone’s domain name as a suffix. For example, the stevens.edu hosted zone may contain records named www.stevens.edu, but not a record named www.stevens.ca. You can use the Route 53 Management Console to create, inspect, modify, and delete hosted zones. You can also use the Management Console to register new domain names and transfer in existing domain names into Route 53’s management.

v) No. The Amazon Route 53 does not have any default value for TTL(time-to-live). TTL specifies the time duration for which DNS resolver caches a response. This must be specified by the user each time.

vi) There is no minimum fee.

Hosted Zones $0.50 per hosted zone / month for the first 25 hosted zones $0.10 per hosted zone / month for additional hosted zones.

The monthly hosted zone prices listed above are not prorated for partial months. A hosted zone is charged upon set-up and on the first day of each subsequent month. To allow testing, a hosted zone that is deleted within 12 hours of creation is not charged; however, any queries on that zone will be charged at the rates below.

Traffic Flow $50.00 per policy record / month A policy record represents the application of an Amazon Route 53 Traffic Flow policy to a specific DNS name (such as www.example.com) in order to use the traffic policy to manage 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.

Standard Queries $0.400 per million queries – first 1 Billion queries / month $0.200 per million queries – over 1 Billion queries / month.

Latency Based Routing Queries $0.600 per million queries – first 1 Billion queries / month $0.300 per million queries – over 1 Billion queries / month.

Geo DNS Queries $0.700 per million queries – first 1 Billion queries / month $0.350 per million queries – over 1 Billion queries / month.

The query prices listed above are prorated; for instance, a hosted zone with 100,000 standard queries would be charged $0.040 and a hosted zone with 100,000 Latency Based Routing queries would be charged $0.060.

Queries to Alias records that are mapped to Elastic Load Balancers, Amazon CloudFront distributions, AWS Elastic Beanstalk environments, and Amazon S3 website buckets are free. Alias records can be created for all query types: standard queries, latency-based routing queries, and geo queries. These queries are listed as “Intra-AWS-DNS-Queries”, “Intra-AWS-LBR-Queries”, or “Intra-AWS-Geo-Queries” on the Amazon Route 53 usage report.

*Sources: Amazon route 53(* [*https://aws.amazon.com/route53/*](https://aws.amazon.com/route53/) *), FAQs(* [*https://aws.amazon.com/route53/faqs/*](https://aws.amazon.com/route53/faqs/) *), AWS Route 53(* [*https://avinetworks.com/glossary/aws-route-53/*](https://avinetworks.com/glossary/aws-route-53/) *)*