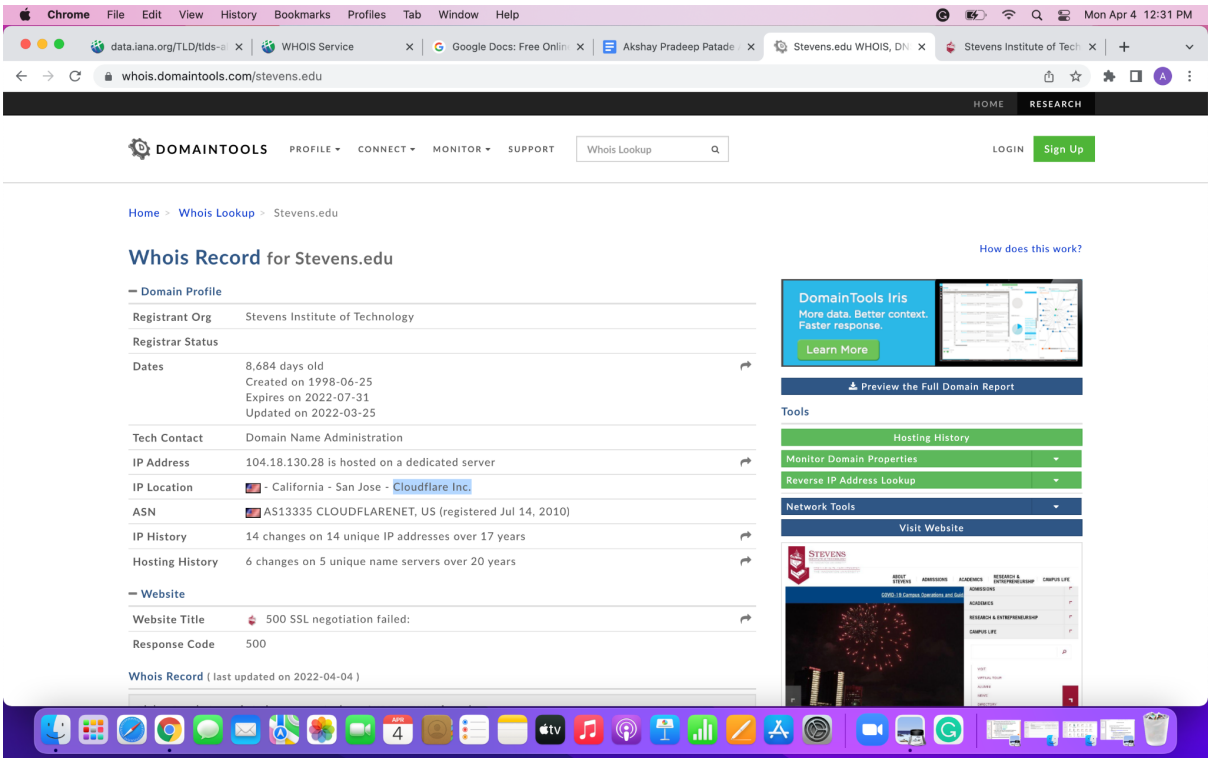
1. There are a total of 1591 domains up to 4th April 2022.

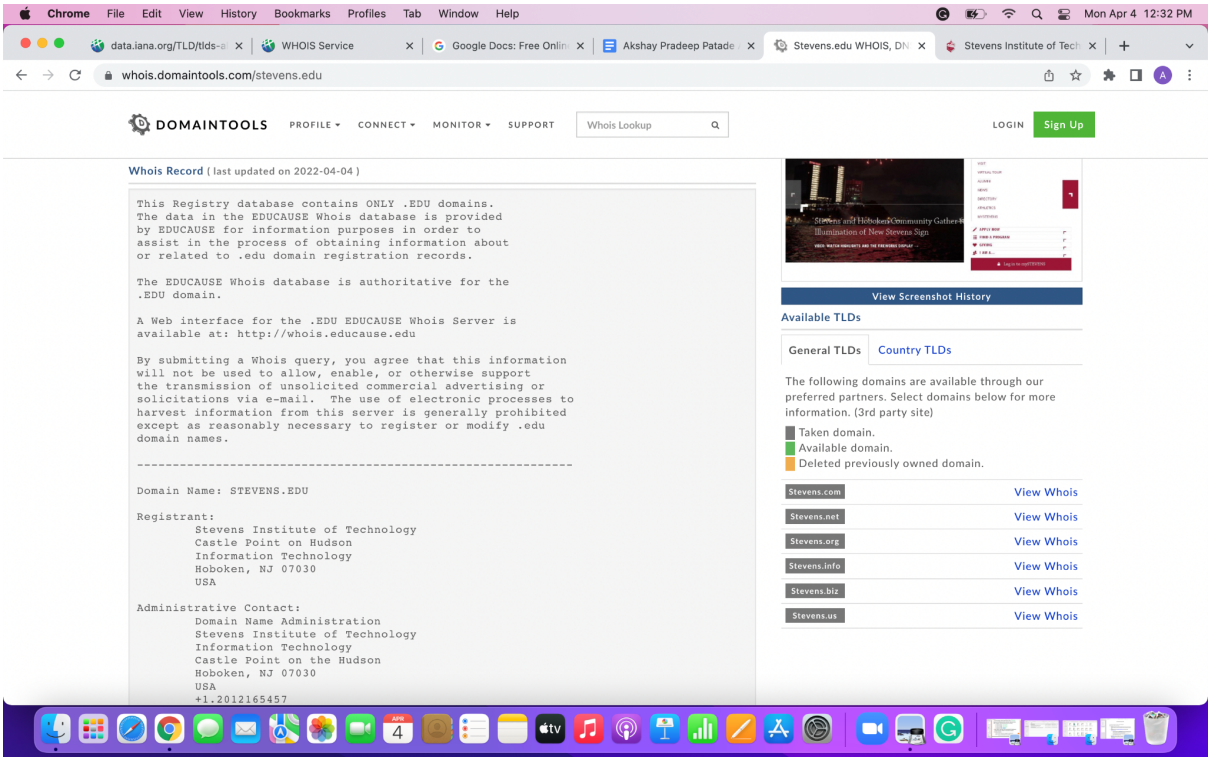
Resource: https://www.iana.org/domains/root/db

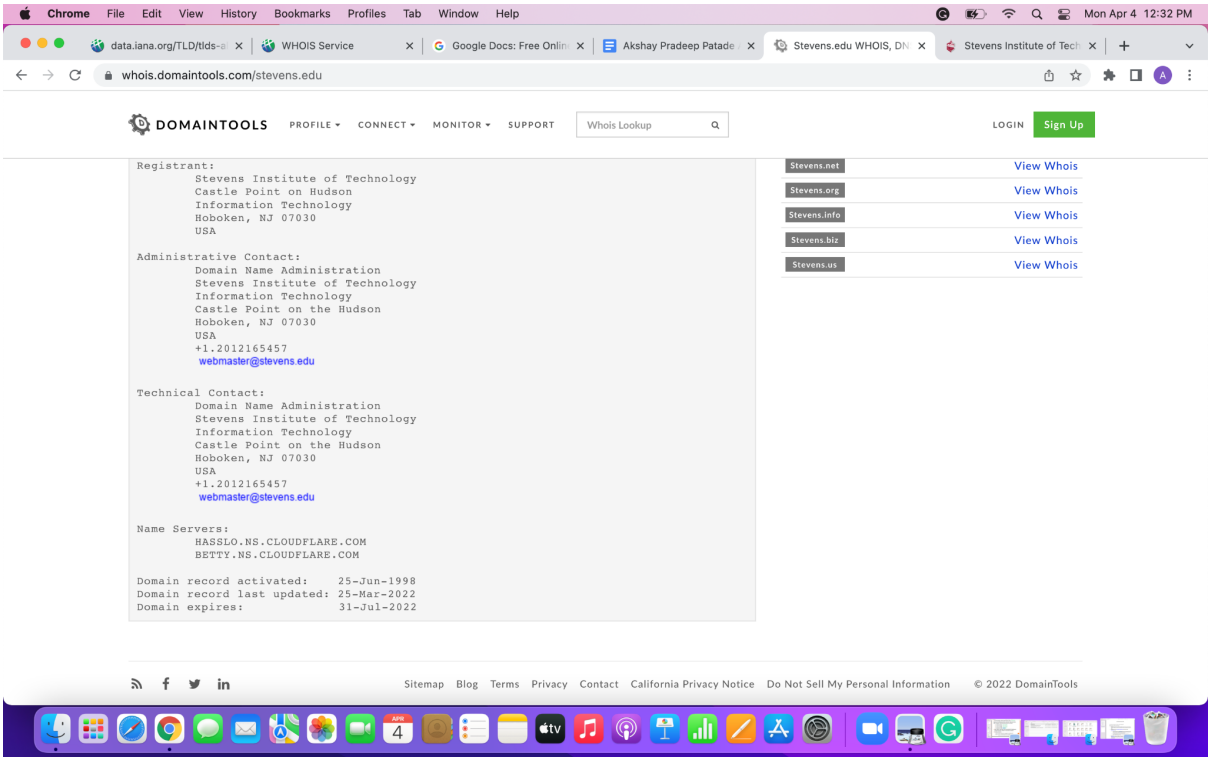
2.

a. Stevens Institute of Technology Domain Information

stevens.edu



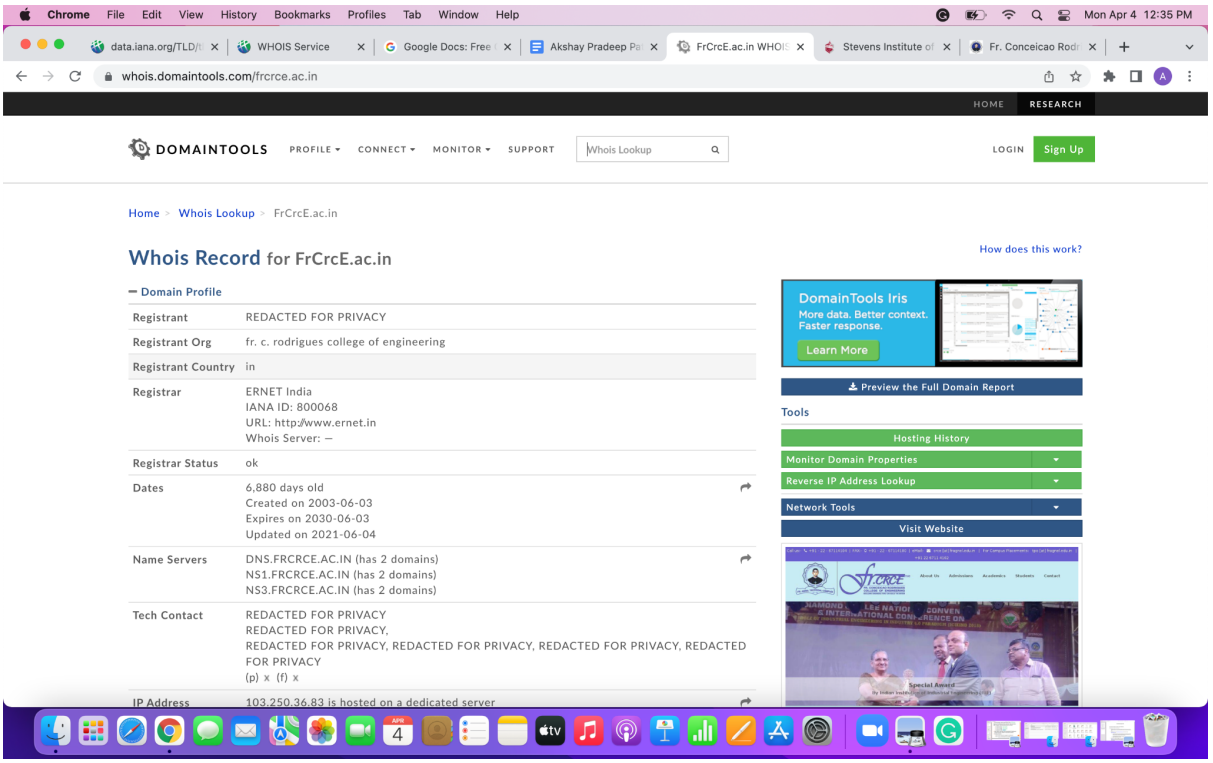


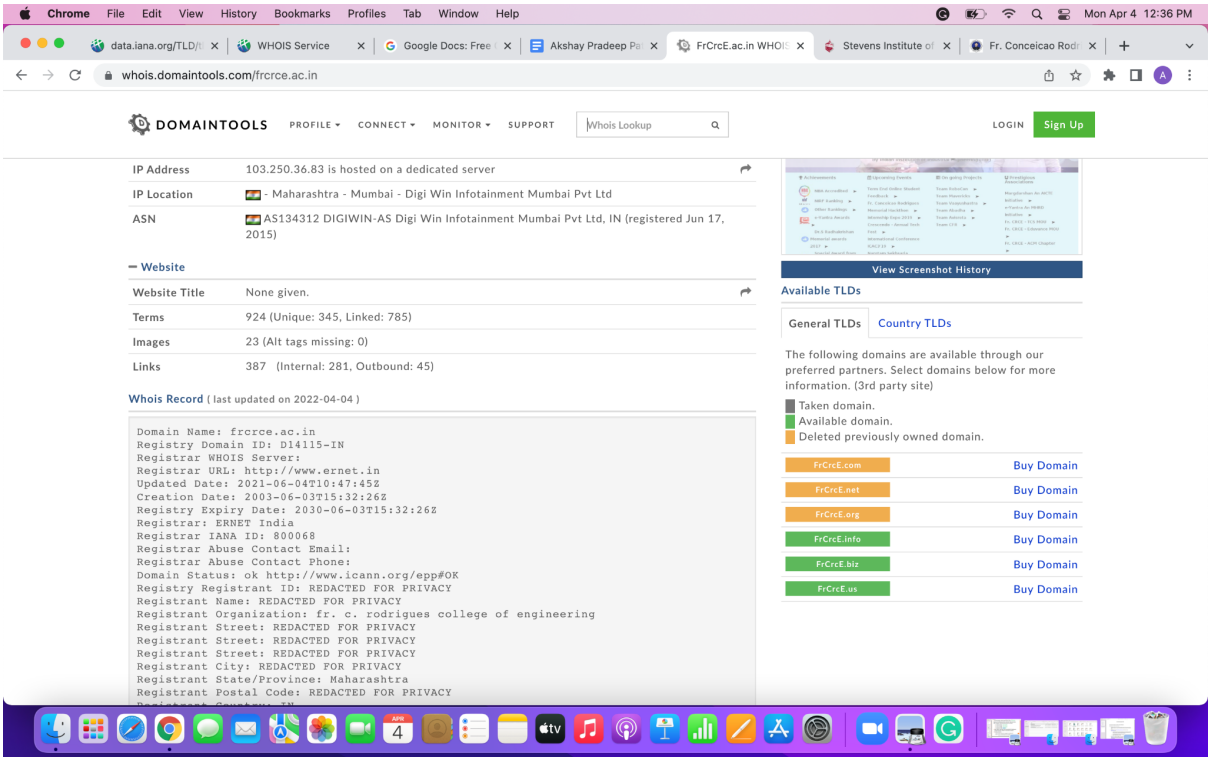


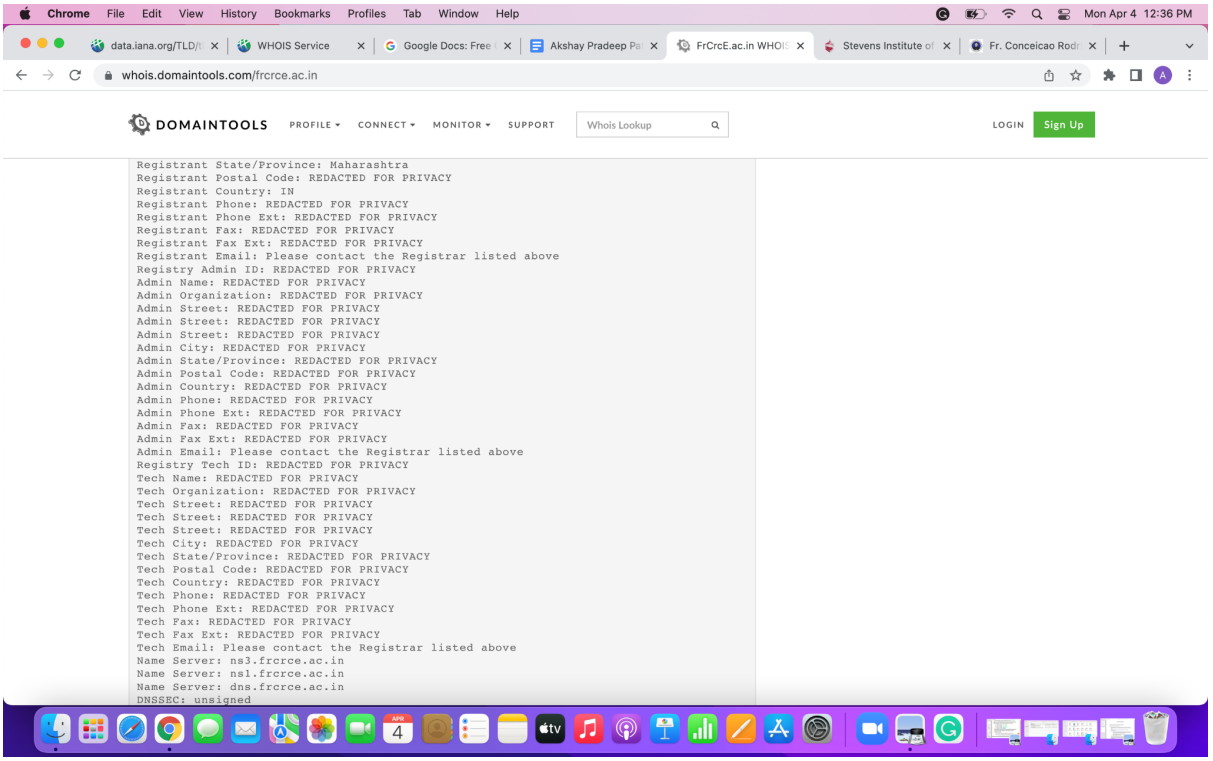
For the Stevens.edu domain, the administrative contact is the Information Technology department of Stevens Institute of Technology.

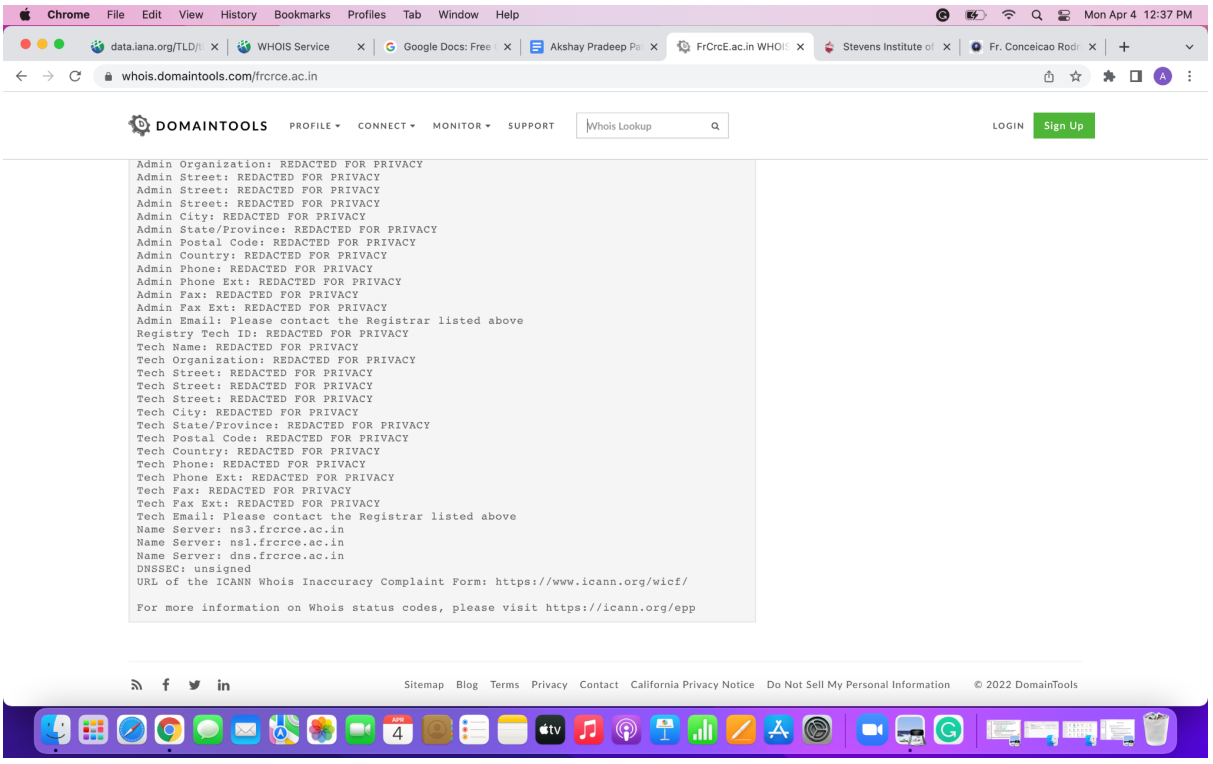
Fr. Conceicao Rodrigues College of Engineering Domain Information

http://frcrce.ac.in/


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon Apr 4 12:35 PM
whois.domaintools.com/frcrce.ac.in
HOME RESEARCH
DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT
Whois Lookup
LOGIN Sign Up
Home > Whois Lookup > FrCrcE.ac.in
Whois Record for FrCrcE.ac.in
How does this work?
Domain Profile
Registrant REDACTED FOR PRIVACY
Registrant Org fr. c. rodrigues college of engineering
Registrant Country in
Registrar ERNET India
IANA ID: 800068
URL: http://www.ernet.in
Whois Server: —
Registrar Status ok
Dates 6,880 days old
Created on 2003-06-03
Expires on 2030-06-03
Updated on 2021-06-04
Name Servers DNS.FRCRCE.AC.IN (has 2 domains)
NS1.FRCRCE.AC.IN (has 2 domains)
NS3.FRCRCE.AC.IN (has 2 domains)
Tech Contact REDACTED FOR PRIVACY
REDACTED FOR PRIVACY,
REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
(p) x (f) x
IP Address 103.250.36.83 is hosted on a dedicated server
DomainTools Iris
More data. Better context. Faster response.
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon Apr 4 12:36 PM
whois.domaintools.com/frcrce.ac.in
DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT
Whois Lookup
LOGIN Sign Up
IP Address 103.250.36.83 is hosted on a dedicated server
IP Location - Maharashtra - Mumbai - Digi Win Infotainment Mumbai Pvt Ltd
ASN AS134312 DIGIWIN-AS Digi Win Infotainment Mumbai Pvt Ltd, IN (registered Jun 17, 2015)
Website
Website Title None given.
Terms 924 (Unique: 345, Linked: 785)
Images 23 (Alt tags missing: 0)
Links 387 (Internal: 281, Outbound: 45)
Whois Record (last updated on 2022-04-04)
Domain Name: frcrce.ac.in
Registry Domain ID: D14115-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2021-06-04T10:47:45Z
Creation Date: 2003-06-03T15:32:26Z
Registry Expiry Date: 2030-06-03T15:32:26Z
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: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: fr. c. rodrigues college of engineering
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Maharashtra
Registrant Postal Code: REDACTED FOR PRIVACY
View Screenshot History
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.
FrCrcE.com Buy Domain
FrCrcE.net Buy Domain
FrCrcE.org Buy Domain
FrCrcE.info Buy Domain
FrCrcE.biz Buy Domain
FrCrcE.us Buy Domain





For frcrce.ac.in, the college has requested the website to not show their administrative contact because of security reasons.

B.

When we try to look at the administrative contact for any. xxx website, they provide the below details.

• Name: Admin Contact
• Organization: ICM Registry LLC
• Email: ops@mmx.co
• Tel: +1 877 734 4783
• Fax: +1 877 809 3183
• Mailing Address: 2505 Second Ave, Suite 520 | Seattle, Washington 98121 United States

3.
The Internet Assigned Numbers Authority (IANA) is a division of the Internet Corporation for assigned names and numbers (ICANN). IANA has the authority of keeping the registries of the Internet unique identifiers that includes Domain Name System (DNS), IPv4 and IPv6 addresses, protocol parameters, and autonomous system numbers. IANA distributes blocks of IP addresses to the five regional internet registries. IANA has various responsibilities such as.

1. To make sure that the creation and assignment of the IP addresses, DNS, and autonomous system numbers are done properly.

2. Ensure that every system uses the same internet parameters and protocols.

3. Taking responsibility for managing the parameters.

ICANN is a nonprofit organization that runs the IANA and makes sure of maintaining several databases related to the namespace of the internet, ensuring the stability and security of the network. ICANN makes sure that all the users on the internet can find valid addresses.

The main difference between ICANN and IANA is that ICANN checks the business and operation-related issues whereas IANA checks the technical issues.

When a business, individual, or government (for the time being we will say entity) buys a domain from the registrar, they have to make sure that they are compliant with the policies imposed by the ICANN and the registrar. The entity is responsible for the registration and use of the domain name. They must respond to the queries raised by the registrar within fifteen days and they should keep their registrar account up to date.

IANA assigns or gives the Domain Name System (DNS), IPv4 and IPv6 addresses, protocol parameters, and autonomous system numbers to the registrar, and then the registrar assigns those to the entity.

The reliability and use of WHOIS data to identify domain registrants have been a difficult subject for the Internet Corporation for Assigned Names and Numbers (ICANN) for years.

WHOIS was designed to be a source of information on domain owners, but it has become a lightning rod for controversy over the years, with much of the blame falling on registrars and

ICANN for failing to adequately crack down on domain owners who have incorrect WHOIS data. ICANN is trying to enhance the process of resolving concerns related to registration data, as it is wary about unscrupulous actors providing fraudulent data to escape detection.

Resources:

https://icannwiki.org/Internet_Assigned_Numbers_Authority

https://www.icann.org/resources/pages/what-2012-02-25-en

https://www.securityweek.com/icanns-rolling-controversy-verification-whois-registration-data

4.

a.
Spamhaus is a nonprofit organization whose objective is to track email spammers and spam-related activity. This company compiles a list of anti-spam lists and various internet service providers and email servers use these lists to reduce the spam that can be sent to their users. On 19th March 2013, Spamhaus has suffered the largest DDoS attack and they took the help of Cloudflare to mitigate this attack. Cloudflare deals with these types of attacks every day.

A major portion of the DDOS traffic directed at Spamhaus is the result of a long-known tactic - a type of reflection attack collectively known as a "DNS amplification assault." Attackers can both multiply the quantity of traffic aimed at a DDOS victim and obscure the source of the attacking machines by relying on the fact that an answer to a DNS query can be substantially greater than the inquiry itself.

The disadvantages of open recursive resolvers:

A DNS server that searches an authoritative nameserver to resolve a domain/address is referred to as a recursive resolver. The open resolver, trusting the faked source address, sends a response to the computer it believes issued the request, which can be hundreds of bytes in size. As a result, the victim's network connection is bombarded with hundreds of bytes of data that were not requested. They will be discarded once they reach the target system, but not before they have used up some of the victim's network capacity. And the traffic that reaches the victim originates from the open resolver, not the computer or machines who launched the assault.

An attacker utilizing a DNS amplification attack can mask the origin of their assault and double the amount of traffic they can direct at the victim by a factor of 40 or more if they have a big list of open resolvers to reflect against. DNS operators who utilize open resolvers without taking safeguards to avoid misuse feel they are doing no damage, but as the Spamhaus DDOS demonstrates, open resolvers may be easily co-opted by attackers and exploited in criminal assaults on third parties.

b.

Spamhaus was suffering from major Layer 3 and minor Layer 4 DDoS Attacks. The main question is what are Layer 3 and Layer 4 attacks? They are two forms of volumetric DDoS assaults on network infrastructure at Layer 3 (network layer) and Layer 4 (transport layer) (transport layer). DDoS assaults employ massive amounts of data (floods) to slow down web server performance, waste bandwidth, and eventually decrease access for genuine users. Typical attack types include ICMP, SYN, and UDP floods.

When an attack occurs, Anycast helps to efficiently dilute it by dispersing it throughout Cloudflare facilities. Because each data center assigns each CloudFlare customer the same IP address, traffic cannot be concentrated in a single area. Instead of being a one-to-one attack, the attack is now one-to-many, with no single point on the network functioning as a bottleneck.

Once the assault has been diffused, it is quite simple to halt at each of CloudFlare's data centers. Because Cloudflare acts as a virtual shield in front of their customers' websites, no attack traffic reaches the customer's servers during Layer 3 attacks. As soon as they joined up for our service, traffic to Spamhaus' network decreased to levels lower than before the onslaught began.

While DNS reflection represented the majority of the traffic involved in the assault, the attacker also used a few other attack tactics. One of them was an ACK reflection attack. A layer 4 attack is ACK reflection. A handshake occurs when a TCP connection is formed. The initiating server sends an SYN (synchronize) request to the receiving server first. The receiving server responds with an acknowledgment (ACK) (for acknowledge). Data can be exchanged after that handshake.

The attacker sends a series of SYN packets to servers with a faked source IP address pointing to the intended victim in an ACK reflection. The servers then send an ACK to the victim's IP address. This, like the DNS reflection attack, disguises the source of the assault by making it appear to be coming from genuine servers. Unlike the DNS reflection attack, however, there is no amplification factor: the bandwidth from the ACKs is symmetrical to the bandwidth available to the attacker to create the SYNs. Unmatched ACKs are dropped by Cloudflare, which mitigates these sorts of attacks.

Resources:
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/

5.

a.
Amazon Route 53 is a cloud Domain Name System (DNS) web service that is highly accessible and scalable. It is intended to provide developers and companies with a highly dependable and cost-effective method of routing end users to Internet applications by translating domain names such as www.example.com into numeric IP addresses such as

192.0.2.1 that computers use to communicate with one another. IPv6 is also fully supported by Amazon Route 53.

Resources:https://aws.amazon.com/route53/

b.
The name AWS Route 53 is derived from Port 53, which handles DNS for both TCP and UDP traffic requests; the phrase Route could relate to routing or a common highway naming scheme. Route 53 is an Authoritative DNS service that stores information about how IP addresses are translated into domain names.

Resources:https://www.bmc.com/blogs/an-introduction-to-aws-route-53/#:~:text=AWS%20Route%2053%20takes%20its,the%20popular%20highway%20naming%20convention.

c.
Amazon route 53 makes sure that the user's requests are effectively connected to the infrastructures running in the AWS such as Amazon EC2 Instances, Amazon Simple Storage Service Bucket (S3), Elastic load balancers, and other AWS services. Amazon route 53 can also be used to route users to infrastructure outside of AWS.

Resources:https://aws.amazon.com/route53/

d.

The term "domain" refers to a DNS concept that applies to all domains. Domain names are instantly recognizable names for numerically addressed Internet sites. A domain is something like amazon.com. Amazon Route 53 provides a concept called the hosted zone. A hosted zone, like a regular DNS zone file, represents a collection of records that can be maintained together and are linked to a single parent domain name. All resource record sets within the hosted zone must have the domain name of the hosted zone as a suffix. For example, records called www.amazon.com and www.aws.amazon.com may exist in the amazon.com hosted zone, but not www.amazon.ca. Use the Route 53 Management Console or API to create, inspect, edit, and delete hosted zones. Alternatively, you can use the Management Console or API to register new domain names and transfer existing domain names into Route 53's management.

Resources: https://aws.amazon.com/route53/faqs/

e.
A variable called the time to live (TTL) associated with each record determines how long a DNS resolver stores a response. There is no default TTL for any record type in Amazon Route 53. For caching DNS resolvers to cache your DNS records for the duration of time provided by the TTL, you must always give a TTL for each record.

Resources: https://aws.amazon.com/route53/faqs/

f.

Like other AWS services, Amazon route 53 follows pay as you go and only for what you use model. There are various pricing aspects for Amazon route 53.

(i) Managing hosted zone: The user has to pay a monthly charge for each hosted zone managed with route 53. User has to pay $0.50 per hosted zone/month for the first 25 hosted zones and after that, they have to pay $0.10 per hosted zone/month for additional hosted zones. Once the hosted zone is created, the user will be charged on the first day of each subsequent month. If a user deletes a hosted zone within 12 hours of creation, they will not be charged. A hosted zone includes 10,000 records. For each record greater than 10,000 per zone, you will be charged $0.0015 per month.

(ii) Serving DNS queries: The user has to pay for every query which is processed by the Amazon route 53 except for the queries which are mapped to the AWS resources such as Elastic Load Balance, Amazon Simple Storage Service Bucket (S3), CloudFront distributions, API Gateways, and VPC endpoints. Queries can be classified into various categories.

Standard Queries: Users are charged $0.40 per million queries for the first 1 Billion queries/month and after that, they are charged $0.20 per million queries.

Latency-based user queries: Users are charged $0.60 per million queries for the first 1 Billion queries/month and after that, they are charged $0.30 per million queries.

Geo DNS and Geoproximity Queries: Users are charged $0.70 per million queries for the first 1 Billion queries/month and after that, they are charged $0.35 per million queries.

(iii) Traffic flow: User is charged with $50.00 per policy record / month. When you associate an Amazon Route 53 Traffic Flow policy with a specific DNS name (such as www.example.com), you generate a policy record, which allows the traffic policy to regulate traffic for that DNS name. The aforementioned monthly price is prorated for partial months. For traffic policies that are not coupled with a DNS name via a policy record, there is no charge.

(iv) Health checks: Route 53 provides basic health checks which charge the users $0.50 per health check/month for AWS services and $0.75 per health check/month.

(v) Resolver Endpoint: Two or more IP addresses are required for a Route 53 Resolver endpoint. One elastic network interface corresponds to each IP address (ENI). Multiple VPCs built by multiple accounts within the same region can share a single outgoing endpoint. Route 53 charges $0.125 per ENI / hour.

Resources:
https://aws.amazon.com/route53/pricing/