Homework 4: CS 524

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.

As of March 2021, the IANA root database includes 1589 TLDs. That also includes 67 that are not assigned (revoked), 8 that are retired and 11 test domains.

(reference: List of Internet top-level domains - Wikipedia)

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?**

ANS.

For Stevens.edu:

Administrative Contact:

Domain Name Administration

Stevens Institute of Technology

Information Technology

Castle Point on the Hudson

Hoboken, NJ 07030

US

+1.2012165457

Some other info:

Dates 8,314 days old

Created on 1998-06-25

Expires on 2022-07-31

Updated on 2021-03-12

It uses cloudflare.

For my undergrad school bvuniversity.edu.in:

It shows most details as “redacted for privacy”

Dates: 4,779 days old

Created on 2008-02-28

Expires on 2027-02-27

Updated on 2020-02-10

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

ANS.

I looked for .xxx TLD which is held by pornographic sites. The information for administrative contact is:

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

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 of it, 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.

DNS Records of Stevens.edu

Name	TTL Until Refresh	Class	Type	Data
www.cs.stevens.edu.	1221	IN	CNAME	www.cs.stevens-tech.edu.
www.cs.stevens-tech.edu. 582665	IN	A	155.246.56.11	

Here the elements are:

NAME is the DNS we looked for.

TTL is Time To Live, or TTL for short, is the sort of expiration date that is put on a DNS record. The TTL serves to tell the recursive server or local resolver how long it should keep said record in its cache. The longer the TTL, the longer the resolver holds that information in its cache. The shorter the TTL, the shorter amount of time the resolver holds that information in its cache.

Class is a static class that retrieves information about a specific host from the Internet Domain Name System (DNS). Here IN is internet and A is address.

CNAME is a Canonical Name record (abbreviated as CNAME record) is a type of resource record in the Domain Name System (DNS) that maps one domain name (an alias) to another (the canonical name)

The www.cs.stevens-tech.edu resolves to 155.246.56.11 address, Its other info is

Country: United States (US)

Region:

City: Hoboken

Latitude :40.7458

Longitude :74.0321

Stevens doesn't specify any of its IPv6 addresses to any hosts but Google does.

(Reference: Understanding TTL Values In DNS Records (ns1.com), CNAME record - Wikipedia)

4. (5 points) Find your machines 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

ANS.

My private IP address at home is 192.168.1.28 and public IP address is 69.120.217.106

```
Server:  sitult.stevens-tech.edu
Address:  155.246.1.20

Name:    ool-4578d96a.dyn.optonline.net
Address:  69.120.217.106
```

DNS Records for: **'69.120.217.106'**

Returned Data

Reverse dns lookup shows this, since I think am connected using Stevens network using VPN.

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.

IANA, the Internet Assigned Numbers Authority, is an administrative function of the Internet that keeps track of IP addresses, domain names, and protocol parameter identifiers that are used by Internet standards. Some of these identifiers are parameters, such as those used by Internet protocols (like TCP, ICMP or UDP) to specify functions and behaviour; some of them represent Internet addresses; and others represent domain names. Regardless of the type of identifier, the IANA function (IANA for short below) ensures that values are managed for uniqueness and made available in publicly-accessible registries so there can be no confusion.

In short, IANA is about managing and ensuring the global uniqueness of three types of Internet identifiers:

a. Protocol parameters

b. Internet Protocol (IP) addresses

c. Internet domain names

ICANN is the Internet Corporation for Assigned Names and Numbers. It is a nonprofit organization headquartered in Southern California that was formed in 1998 to help the U.S. government manage certain functions that maintain the Internet's core infrastructure. ICANN maintains the central repository for IP addresses and helps coordinate the supply of IP addresses. It also manages the domain name system and root servers. ICANN currently manages over 180 million domain names and four billion network addresses across 240 countries. It is also important to note that which ICANN does not control, such as content on the Internet, malware or spam and Internet access. IANA is a part of ICANN.

- 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.

Difference between IANA and ICANN:

IANA – Internet Assigned Numbers Authority, a part of ICANN that performs technical services critical to maintaining the DNS

ICANN currently gets its authority to manage the DNS via the IANA contract, granted to them by the U.S. government, but that would change under the proposed plan.

The Whois Controversy:

For years, the Internet Corporation for Assigned Names and Numbers (ICANN) has had a thorny issue to contend with – the accuracy and use of WHOIS data to identify domain registrants.

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. Wary of bad actors supplying false data to avoid detection, ICANN however is hoping to improve the process of resolving issues tied to registration data.

According to Felman, the contentiousness of the issue comes down to competing interests. On the one hand are privacy and free speech advocates concerned that WHOis data can be used for repression, and on the other hand is the law enforcement and business communities, who are concerned with tracking down counterfeiters and others. This has become a source of controversy as the new RAA is being negotiated, he said.

Proposed elimination of public DNS whois

In 2013, the initial report of ICANN's Expert Working Group has recommended that the present form of Whois, a utility that allows anyone to know who has registered a domain name on the Internet, should be "abandoned". It recommends it be replaced with a system that keeps most registration information secret (or "gated") from most Internet users, and only discloses information for "permissible purposes". ICANN's list of permissible purposes includes domain name research, domain name sale and purchase, regulatory enforcement, personal data protection, legal actions, and abuse mitigation. Whois has been a key tool of investigative journalists interested in determining who was disseminating information on the Internet. The use of whois by journalists is not included in the list of permissible purposes in the initial report.

(References: IANA Functions: The Basics | Internet Society, ICANN - Wikipedia, What Is ICANN and Why Does It Matter? | Data Foundry, ICANN's Rolling Controversy: Verification of WHOIS Registration Data | SecurityWeek.Com)

6. (50 points) The Spamhaus attack

a. (5 points) Read https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal conspiracy-2/ . Describe (in no more than a couple of paragraphs) the Spamhaus attack and explain the dangers of open recursive resolvers.

ANS.

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.

To accomplish this, 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.

Because most DNS traffic is stateless by design, an attacker could start a DoS attack in the following way:

1. The attacker starts by configuring a record on any zone he has access to, normally with large RDATA and Time to Live (TTL).

2. Taking advantage of clients on non-BCP38 networks, the attacker then crafts a query using the source address of their target victim and sends it to an open recursive nameserver.

3. Each open recursive nameserver proceeds with the resolution, caches the record, and finally sends it to the target. After this first lookup, access to the authoritative nameservers is normally no longer necessary. The record will remain cached at the open recursive nameserver for the duration of the TTL, even if it's deleted from the zone.

4. Cleanup of the zone might, depending on the implementation used in the open recursive nameserver, afford a way to clean the cached record from the open recursive nameserver. This would possibly involve queries luring the open recursive nameserver to lookup information for the same name that is being used in the amplification.

Because the characteristics of the attack normally involve a low volume of packets amongst all the kinds of actors besides the victim, it's unlikely any one of them would notice their involvement based on traffic pattern changes.

Taking advantage of an open recursive nameserver that supports EDNS0, the amplification factor (response packet size / query packet size) could be around 80. With this amplification factor, a relatively small army of clients and open recursive nameservers could generate gigabits of traffic towards the victim.

(References: Is Your Open DNS Resolver Part of a Criminal Conspiracy? - ISC, https://www.ietf.org/rfc/rfc5358.txt)

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.

Distributed denial-of-service campaigns have been making headlines with disturbing frequency, namely from the large attack on Spamhaus that peaked at 300 Gbps. This attack allegedly had no effect on customers, according to the group, but this should serve as a data security warning to companies that do not have protections in place against a DDoS or similar cyberattack, according to InformationWeek editor Matthew Schwartz.

The attack didn't happen all at once, according to The New York Times, as it first started with about 1,000 computers which were pretending to be Spamhaus and sending information to an open domain name resolver . Spamhaus was not able to handle that amount of traffic, as for each message that was sent to the server, they replied with a message 100-times larger than the initial request.

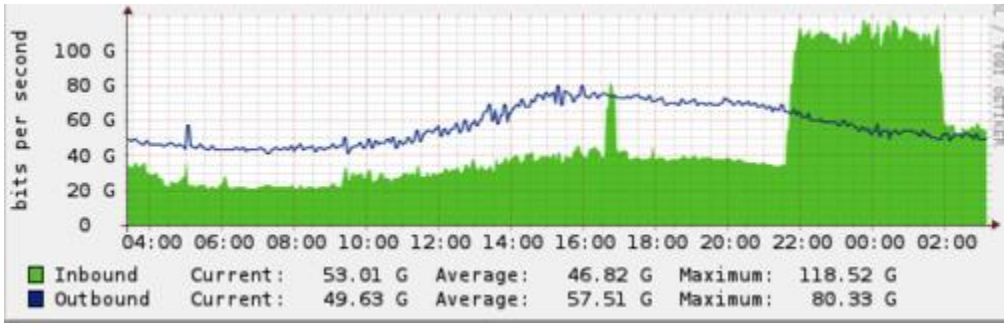
Beginning on March 18, the Spamhaus site came under attack. The attack was large enough that the Spamhaus team wasn't sure of its size. It was sufficiently large to fully saturate their connection to the rest of the Internet and knock their site offline. These very large attacks, which are known as Layer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

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: Leveraging lessons from Spamhaus to stop DDoS attacks - (trendmicro.com), https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/)

7. (20 points) Study the Amazon Route 53 service and answer the following questions

a. What does Route 53 do?

ANS.

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 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 in order to enable a variety of low-latency, fault-tolerant architectures. 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. 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.

Benefits:

- Highly available and reliable
- Flexible
- Designed for use with other Amazon Web Services
- Secure, Simple and fast

(References: Amazon Route 53 - Amazon Web Services)

b. Why is it called Route 53?

ANS.

AWS Route 53 takes its name with reference to Port 53, which handles DNS for both the TCP and UDP traffic requests; the term Route may signify the routing, or perhaps the popular highway naming convention. Route 53 is an Authoritative DNS service, which contains information about the mapping of IP addresses to domain names.

(References: An Introduction to AWS Route 53 – BMC Software | Blogs)

c. What other Amazon services is it designed to work with (please explain how it happens with one or two examples)?

ANS.

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, API Gateway, VPC endpoint, or Amazon S3 website bucket using a feature called Alias record.

AWS CloudTrail

Amazon Route 53 is integrated with AWS CloudTrail, a service that captures information about every request that is sent to the Route 53 API by your AWS account. You can use information in the CloudTrail log files to determine which requests were made to Route 53, the source IP address from which each request was made, who made the request, when it was made, and so on.

Amazon CloudFront

To speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website—including dynamic, static, streaming, and interactive content—by using a global network of edge locations. CloudFront routes requests for your content to the edge location that gives your users the lowest latency. You can use Route 53 to route traffic for your domain to your CloudFront distribution.

(References: Amazon Route 53 - Amazon Web Services, Integration with other services - Amazon Route 53)

d. What is the difference between the domain name and hosted zone?

ANS.

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 existing domain names into Route 53's management.

(References: Amazon Route 53 FAQs - Amazon Web Services)

e. Does Route 53 have a default for the Time-to-live (TTL) value?

ANS.

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. 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.

(References: Amazon Route 53 FAQs - Amazon Web Services)

f. What is the pricing of the service?

ANS.

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:

- Managing hosted zones: You pay a monthly charge for each hosted zone managed with Route 53.
- 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.
- 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.

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.

Alias Queries

Queries for qualifying alias records are provided at no additional cost to Route 53 customers.

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.

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

DNSSEC

Amazon Route 53 does not charge you to enable DNSSEC

Public DNS Query Logs

Amazon Route 53 does not charge for public DNS query logs

(References: Amazon Route 53 pricing - Amazon Web Services)