Answer01:

As of April 3, 2024, There is an approximate number of 1448, this information is provided on the website https://data.iana.org/TLD/tlds-alpha-by-domain.txt.

Answer02:

a. The table shows the information of stevens.edu (Grad School), and abebooks.com (Random Website for buying/selling of books)

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	Admin Name: Hannes Blum Admin Organization: Abebooks Inc. Admin Street: 5th Floor, 655 Tyee Road Admin City: Victoria Admin State/Province: BC Admin Postal Code: V9A 6X5 Admin Country: CA Admin Phone: +1.2504123200 Admin Phone Ext: Admin Fax: +1.2504756014 Admin Fax Ext: Admin Email: domains@abebooks.com

b. Administrative contact for .xxx domain

```
Registry Admin ID: REDACTED FOR PRIVACY
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 query the RDDS service of the Registrar of Record
identified in this output for information on how to contact the
Registrant, Admin, or Tech contact of the queried.
```

All the contact information of Admin is hidden to maintain privacy.

Answer03:

Structures and Responsibilities of IANA:

The Internet Assigned Number Authority (IANA) is an ICANN (non-profit American Corporation) sub department. It is responsible for maintaining and assigning unique codes used for the technical standard.

It can be broadly grouped into:

- Domain Names
- Number Resources
- Protocol Assignment

Structures and Responsibilities of ICANN:

It is an organization formed by different interest groups of the internet and jointly contribute to any final divisions of ICANN's make. There are few supporting organizations with their roles and responsibilities as under:

- Three Supporting Orgs responsible for IP Address, Domain Name. and Country-Code Management.
- Four Advisory Committee for recommendations and advising.
- Technical Liaison Group to coordinate basic internet technologies protocol.

Following are some of the role's ICANN plays in the world of the Internet.

- Consideration and Implementation of Top-Level Domain (TLD).
- Relationship formalization with root name server operators.
- Contingency Planning.
- Information Sharing for promotions of best-practices throughout the industry.
- Conduct Reviews and necessary administrative structural changes.

Difference in responsibilities between IANA and ICANN:

- IANA runs Top-level Domains, ports and IP Address Management whereas ICANN is a non-profit cooperation responsible for managing internets worldwide space.
- IANA runs TLDS, and ICANN is an organization that runs IANA on grounds of an MoU.

Controversy in ICANN Concerning Whois:

ICANN was found pushing a plan to restrict public access to Whois database based on the reasoning that it is publicly accessible, no one can be held accountable for the patterns of usage of that database.

Therefore, ICANN proposes a solution to scrap the existing Whois database and formulate a new structure which is closed by default and would only be made accessible to the authenticated requestor.

Answer04:

a. Spamhaus was targetted as one of the attacks which utilize Distributed Denial of Service (DDoS).

   The attackers exploited a loophole in the DNS system to carry out the attack. Fake request in huge numbers were initiated by the attackers to thousands of open resolvers which resulted in huge replies being parsed at the Spamhaus Servers.

   Open Recursive Resolvers are DNS servers that responds to queries originating from any internet connected device. Such connectivity allows room for a significant security threat which can possibly lead to its exploitation by performing DNS amplification.

b. The Spamhaus site came under attack on March 18. The attack intensity was not sure to the Spamhaus team, but apparently large enough to exhaust the resource capacity of Spamhaus network infrastructure causing their dysconnectivity to the internet and it went offline. The entire attack was an L3 attack where attack was launched from a number of compromised sources simultaneously creating huge network load on Spamhaus server (upto 120Gbps peak hit).

   How the internet works is large organizations like CloudFlare, google, bandwidth providers like At&T, Level3, and Cogent run networks. These independent network are paired with each other to provide a broad connectivity. CloudFlare is connected to mostly all networks, and due to their connectivity, it helped blocked all the malicious requests routing towards Spamhaus servers. The CloudFlare connects to the majors networks using two different strategies, one is with a typical Fiber Optics cable connection between routers placed at the border of each network, the second is connection with an Internet Exchange, IXs for short.

   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 customers sites, with Layer 3 attacks none of the attack traffic reaches the customer's servers. Traffic to Spamhaus's network dropped to below the levels when the attack started as soon as they signed up for our service.

   Ref: (https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet)

Answer05:

Amazon R53 is a DNS web service.

a. Allows you to register/transfer domains. It basically provides the services of domain name to IP addresses mapping.
b. Because it utilizes port 53 of TCP/UDP to resolve DNS queries.
c. It is designed to work with a lot of AWS Services. It can be used to map a load balancer to a domain name, make an ECS application accessible via a domain name, It can also be used to enable route forwarding. It can also be used to configure make s3 objects accessible via a domain.
d. Domain Name is a general human readable representation of any IP address. Whereas Hosted Zone represent a group of DNS name which can be managed together can falls under one hosted zone file. It is a logical isolation of your domain records under one common group.
e. No, R53 services do not have a default TTL, you must manually provide a TTL for any record.
f. There is no minimum pricing however;

   Hosted Zone:

   $0.50 per hosted zone (for the first 25), and $0.10 for additional hosted zone (above 25)

   Queries:

- Standard Queries:
  - $0.40W per million queries (first 1 Billion Queries/month)
  - $0.20 per million (over 1 Billion Queries/month)
- Latency Based Routing Queries:
  - $0.60 per million queries (first 1 Billion Queries/month)
  - $0.30 per million (over 1 Billion Queries/month)
- Geo DNS and Geo-proximity Queries:
  - $0.70 per million queries (first 1 Billion Queries/month)
  - $0.35 per million (over 1 Billion Queries/month)
- IP Based Querying:
  - $0.80 per million queries (first 1 Billion Queries/month)
  - $0.40 per million (over 1 Billion Queries/month)

Traffic Flow:

$50.00 per policy record/month

Health Check:

Basic Health Check:

$0.50 per health check/month (AWS Endpoint)

$0.75 per health check/month (Non-AWS Endpoint)

Optimal Health Check Features: HTTPS, String Matching, Fast Interval, Latency Measurement:

$1.00 /month per optional feature (AWS Endpoint)

$2.00 /month per optional feature (Non-AWS Endpoint)

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