Tutorial 7: Governance of the Internet

1. Compare the top-level domains (TLD) and country-code top-level domains (ccTLD) by giving appropriate examples. (PIC: Pei Xuan)

Subset of TLD :

- gTLD – Generic Top-Level Domains
  E.g. com, edu, org. gov, net (organizations involved in networking technologies or established network for multiple to join/share/link across)
- sTLD – Sponsored Top-Level Domains
  E.g. .travel, .boutique, .museum
- ccTLD – Country Code Top-Level Domains
  E.g. .au (Australia),.my,.sg,.id(Indonesia)

-iTLD -infrastructure TLD
E.g. .arpa (used for internet infrastructure development & research purpose)

Top-level domains (TLD)	**Country-code top-level domains (ccTLD)**
A Top Level Domain (TLD) is the part of the domain name located to the **right of the dot (" . ")** →made up of the rightmost part of a domain name.	Country-code TLDs (ccTLDs) represent specific **geographic locations**
A TLD (top-level domain) is the most generic domain in the Internet's hierarchical DNS (domain name system)	Country-code top-level domains (ccTLD) is one of type of Top-level domains (TLD)
Example: .com, .net, and .org. Some others are .biz, .info, and .ws	Example: .my represent Malaysia, .eu represent European Union, .us represent United State

2. With the use of example, compare and contrast the following:
• Domain name hijacking
• Reverse domain name hijacking
• Typosquatting

(PIC: Xin Yi)

Domain name hijacking

Registration of well known names for the purposes of selling them for profit, or to redirect traffic looking for other organizations to one's own site

Domain name hijacking is when a hacker wrongfully gains control of their target's complete Domain Name System (DNS) information, enabling them to make unauthorized changes and transfers to their advantage. The easiest and most common way is by changing the administrator's handle information through social engineering or hacking into the administrator's email account. The first piece of information that an attacker needs to access their targets' domain control panels is the administrative contact email address.

Example:

1. Companies are vulnerable to new content put on their site, and this can result in severely damaging their reputation, and the loss of customers. A recent example of pharming hijacking is when Air Malaysia's domain name was hijacked and replaced with a picture of pipe smoking, monocled lizard.

2. Joe plans in advance that proton.com.my would be a valuable www address name. He will purchase this domain name earlier than proton company. If the proton company wants to use this domain name, they need to pay money for him.

Reverse domain name hijacking

- Attempts to use **legal processes** to grab a legitimate name that an organization simply wished it had the foresight to register first has become known as and is arguably as big a problem as domain-name hijacking.

Example:

1. Joe bought the domain name but he does not use the domain name to make profit upon sale. However, his family uses it for pictures and blogs. It may cause the Proton company to decide to sue Joe and be required for monetary compensation.

Typosquatting

- Typosquatting is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites. Users may be tricked into entering sensitive details into these fake sites. For organizations victimized by these attackers, these sites can do significant reputational damage. Hackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes.

Example:

1. Most attackers will make use of the website for the purpose of phishing. These websites will have identical interfaces as the original website so visitors will feel safe to enter confidential information such as login, passwords or banking details. As such, hackers will collect that information not only granting access to the typosquatting site, but also other popular websites in the case of the victim using the same login credentials.

2. Joe as the typosquatter buys mispelled domain names/URLs such as gougle.com, Roogle.com to get visits from internet users who mistyped the name of the popular website "Google.com". This may end up giving chances for these typosquatted website to retrieve sensitive information from the visitors such as username, password or bank account details.
3. Leading to Non-malicious objective/intention-Typosquatting attacks also were used by businesses in promoting their product and services. For example, typing www.goooogle.com will redirect users to another website that advertised investment services, news and advice.

3. Many trademark holders were quite slow off registering their trademark as a second-level domain in the .com, **resulting in domain name hijacking**. Using appropriate examples, discuss two problems caused by domain name hijacking and one legal way to grab the domain name. (PIC: Jun Xian)

Problems:

1. **Information theft**
When the hackers have hijacked the domain name, they can access the traffic of the domain. Thus, they can access confidential information such as bank accounts, passwords of the customers who are visiting the website.

2. **Revenue lost**
Hackers who hijacked an existing domain of a business website can redirect the website visitors to a fake website or transfer the ownership of the domain name to others. This is especially dangerous for e-commerce businesses as when the domain name is stolen, the e-commerce system will no longer be working and cause the business to lose revenues.

Ways to tackles problem issue mentioned above/legal way to grab the domain name:

1. To grab the domain name is through **Reverse Domain Name Hijacking** which refers to a situation where one company who claims that they own the trademark can go through a legal process and take legal action to get back their domain name.

2. Legal way to purchase, **purchase through reliable and trustable parties** such as Google Domain, GoDaddy, www.whoisnet and avoid using a domain name which is similar to a trademark name.

4. What is ICANN? Explain any THREE (3) the role of ICANN under Internet governance. (PIC: Kah Wei)

ICANN (Internet Corporation for Assigned Names and Numbers) is an internationally organized, non-profit partnership of people from all over the world dedicated to keeping the internet secure, stable and interoperable. It promotes competition and develops policy on the internet's unique identifier.

The first role of ICANN is it **provides a stable environment for the domain name system** (DNS). It does this by making sure that a website with the same domain name is not sold to two people at the same time through the contracts with the registries. And that people browsing the internet can quickly find the websites they are looking for, because they have unique Domain Names (DNs).

The second role is ICANN ensures that the **IP address assigned to each domain name is recognizable** by the computers and other devices in order to prevent clashes or confusion of having the same IP address issued to the same website.

The third role of ICANN is ICANN ensure that the **internet remains updated** as new technologies or advancements are recorded in the field with the collaboration of 13 root servers all over the world.

-help coordinate the supply of IP addresses and maintain the central repository for IP addresses.

-manages the namespace of the **internet and root servers**. E.g. manages the Internet Protocol address spaces for IPv4 and IPv6,

-Beside that, ICANN **ensures the stability of the networks** and **secure operation** such as protect content on the internet, prevent malware or spam attack and proper internet access.

-Therefore, ICANN according to the function contract of Internet Number Assignment Agency (IANA) performs the actual technical maintenance of the Central Internet Address pool and

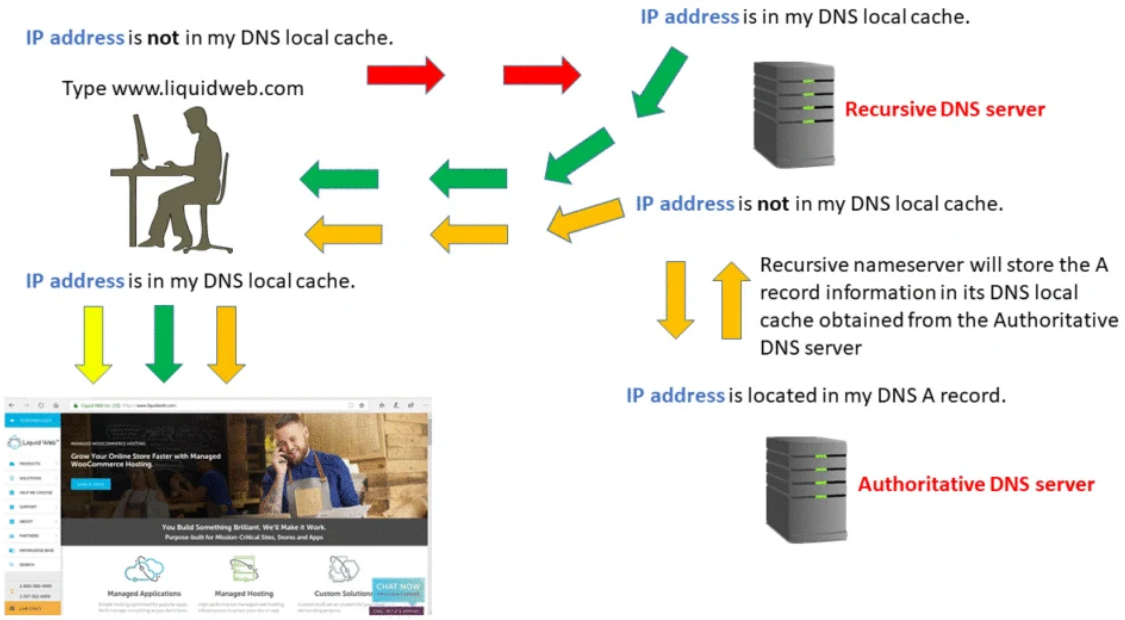
Domain Name System(DNS) root domain registry.

-responsible for coordinating the management of the technical elements of the DNS to ensure universal resolvability so that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique technical identifiers used in the Internet's operations, and delegation of Top-Level Domain names (such as .com, .info, etc.) among different regional internet registries and release new TLD into the market (e.g .boutique, .museum, .travel, .mobile….etc)

In conclusion, ICANN involved itself in draft , finalized and enforce Internet governance related rules/policy/terms and conditions.

5. Watch this YouTube video clip, then explain how Domain Name Server (DNS) works. You may include appropriate diagrams in your answer.
Ref: https://www.youtube.com/watch?v=mpQZVYPuDGU (PIC: Yit Wee)

DNS translates domain names to IP addresses so browsers can load Internet resources. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168



Step 1: Requesting Website Information

Let's visit a website by typing a domain name into a web browser. Our computer will start resolving the hostname, such as www.liquidweb.com. Our computer will then look for the IP address associated with the domain name in its local DNS cache. This cache stores this information that our computer has recently saved. If it is present locally, then the website will be displayed. If our computer does not have the information, it will perform a DNS query to retrieve the correct information.

Step 2: Contact the Recursive DNS Servers

If the information is not in your computer's local cache, then it will query another server. Recursive DNS servers have their local cache, much like your computer. Many ISP's use the same recursive DNS servers, it's possible that a common domain name is already in its cache. If the domain is cached, the query will end here and the website will be displayed to the user.

Step 3: Query the Authoritative DNS Servers

If a recursive DNS server or servers do not have information stored in its cache memory, it looks elsewhere. The query then continues up the chain of authoritative DNS servers. The search will continue until it finds a nameserver for the domain. These authoritative name servers are responsible for storing these records for their respective domain names.

Step 4: Access the DNS Record

To locate the IP address for liquidweb.com, we will query the authoritative name server for the address record (A record). A Recursive DNS server accesses the A record for liquidweb.com from the authoritative name servers. It then stores the record in its local cache. If another query requests the A record for liquidweb.com, the recursive server will have the answer. All DNS records have a time-to-live value, which shows when a record will expire. After some time has passed, the recursive DNS server will ask for an updated copy of the records.

Step 5: Final DNS Step

The Recursive DNS server has the information and returns the A record to your computer. Our computer then stores the record in its local cache. It reads the IP address from the DNS record

and passed it to our browser. The web browser will connect to the web server associated with the A records IP and display the website.

The entire lookup process, from start to finish, takes only milliseconds to complete. For a better understanding, let's break down the components that make up the lookup process.

6. Discuss the importance of internet users to care about Internet Governance. Then differentiate the TWO (2) common types of Internet governance models: multi-stakeholder versus multi-lateral models. (PIC: Chia Chung)

The major importance of internet users to care about Internet Governance is privacy/security issues. It has a direct effect on journalists where the sources they have must be anonymous, which means the Internet Governance has to keep internet users away from surveillance. On the other hand, we also have a lot of governments that like to collect information and data about their citizens.

Multi-stakeholder	**Multi-lateral**
Refers to the heart of the Internet ecosystem .	Refers to discussion or agreements between multiple governments
Reflects the commitment to an open dialog between governments, private sector organizations, civil society and technical community.	Does not provide for the inclusion of other communities that have been part of the multistakeholder process.
High degree of transparency.	Low degree of transparency.
The USA, France, England etc	Canada, Australia, Switzerland, China etc.
Decision Maker: Multistakeholder committee comprises of following parties:	Decision Maker: - Individual government - Discussion between two or more

- NGO - Government - Private sector - Public - Civil society - Education sector - Etc. -To meet up, draft, discuss, debate and finalized the internet governance policy and enforcement Countries: France, USA, south korea, etc	governments - In order to draft, discuss and finalize the internet governance policy and enforcement. Countries: China, North korea
Low degree of web surveillance/web content censorship	High degree of web surveillance/web content censorship