Domain Name System Protocol

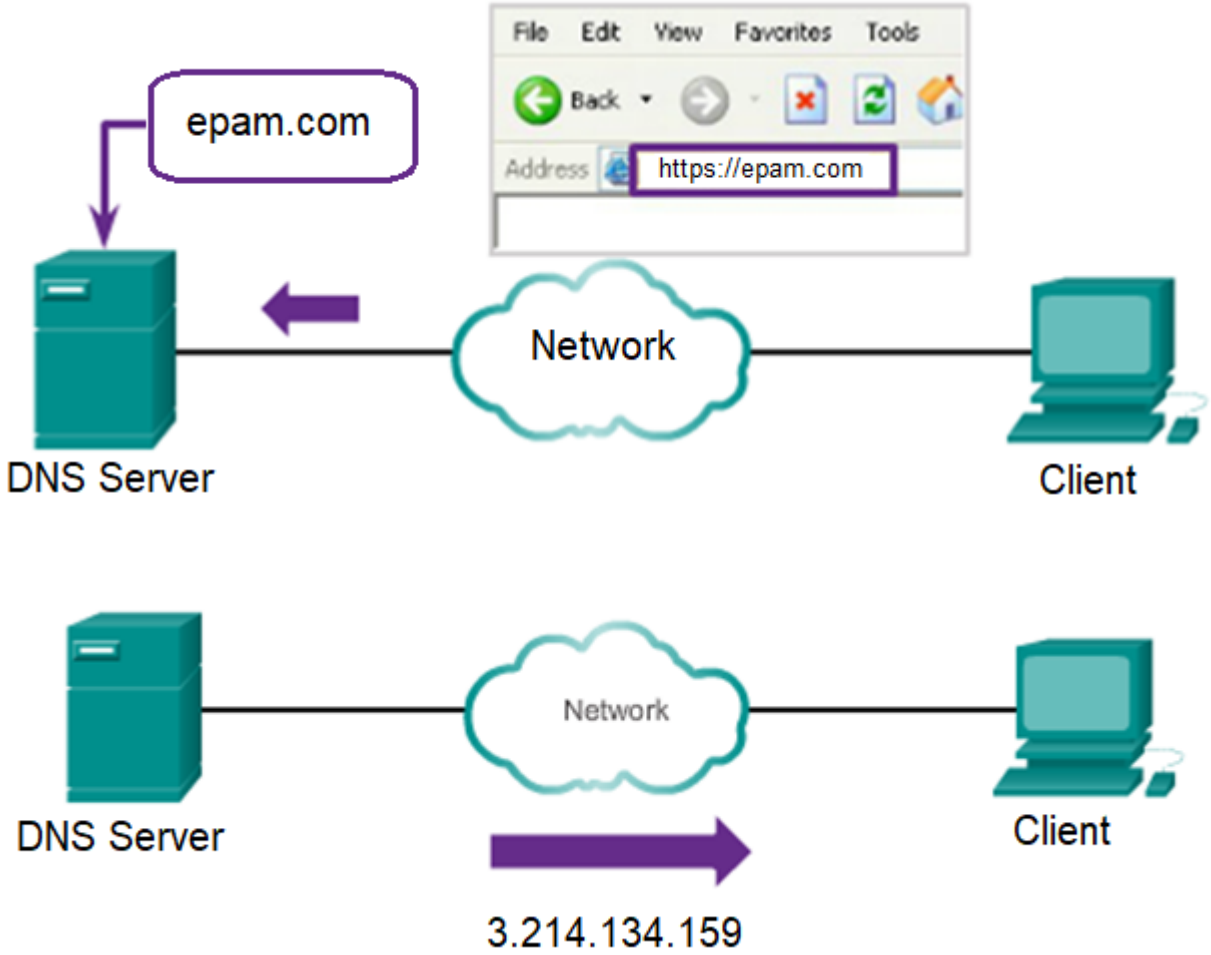
Serhii Zakharchenko

Agenda

- DNS basics
- DNS server types
- Name resolving process overview
- DNS records
- DNS security

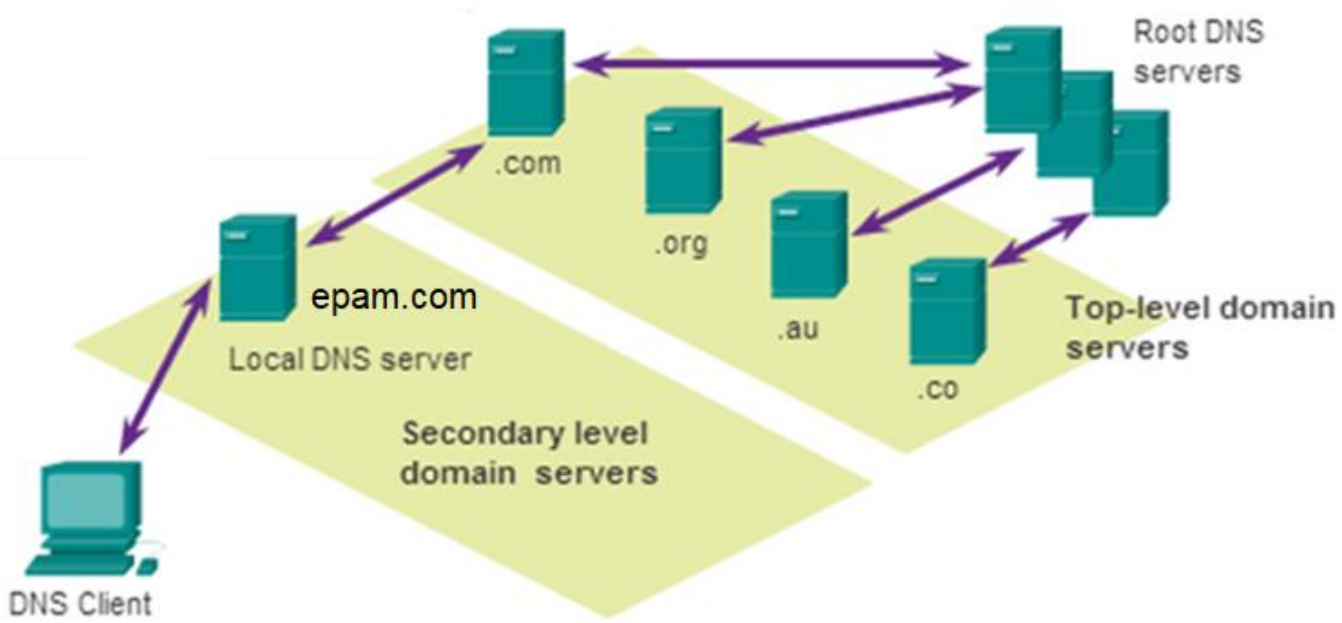
Domain Name Service

- The Domain Name System (DNS) was created for **domain name to address resolution** for these networks.
- DNS uses a **distributed set of servers** to resolve the names associated with these numbered addresses.
- The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data.



Domain Name Space

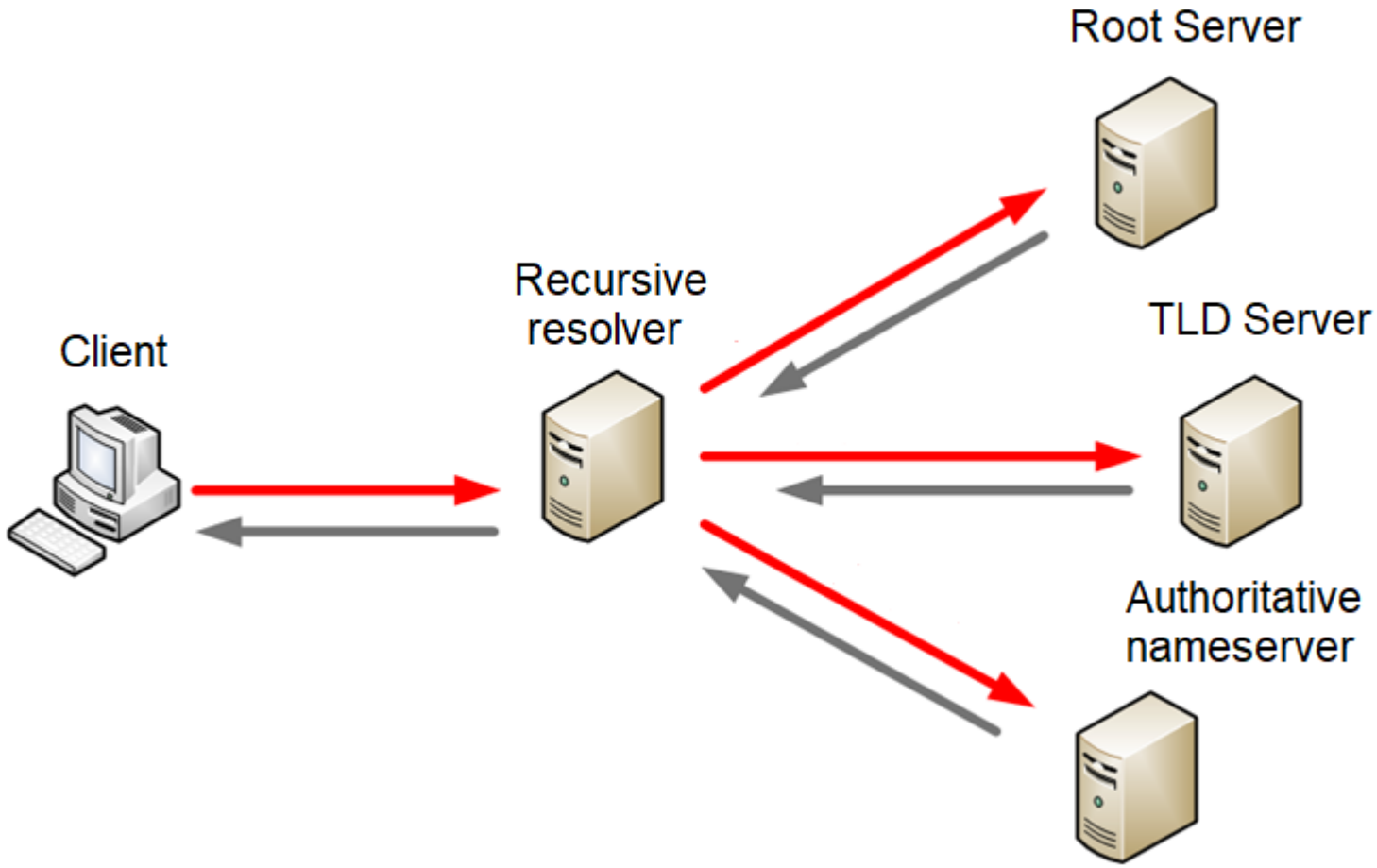
- DNS uses a hierarchy to manage its distributed database system.
- The DNS hierarchy, also called the **domain name space**, is an inverted tree structure.
- The DNS tree has a single domain at the top o the structure called the root domain. A period o dot (.) is the designation for the root domain.



- While searching for a host, the DNS tree is traversed in an ascending order, starting from leaf nodes and moving towards the root. Therefore, the nodes falling on the left side are more specific in contrast to the nodes on the right side. For example, node epam in epam.com is more specific than the com node.
- In a **Fully Qualified Domain Name** (FQDN), the host name is specified by the leftmost label. The next label to the right defines the local domain to which the host belongs. The local domain also can be a part of or a sub-domain of another domain. Therefore, naming gets less specific while moving from the left to the right. This process is followed until the root of the tree is reached.

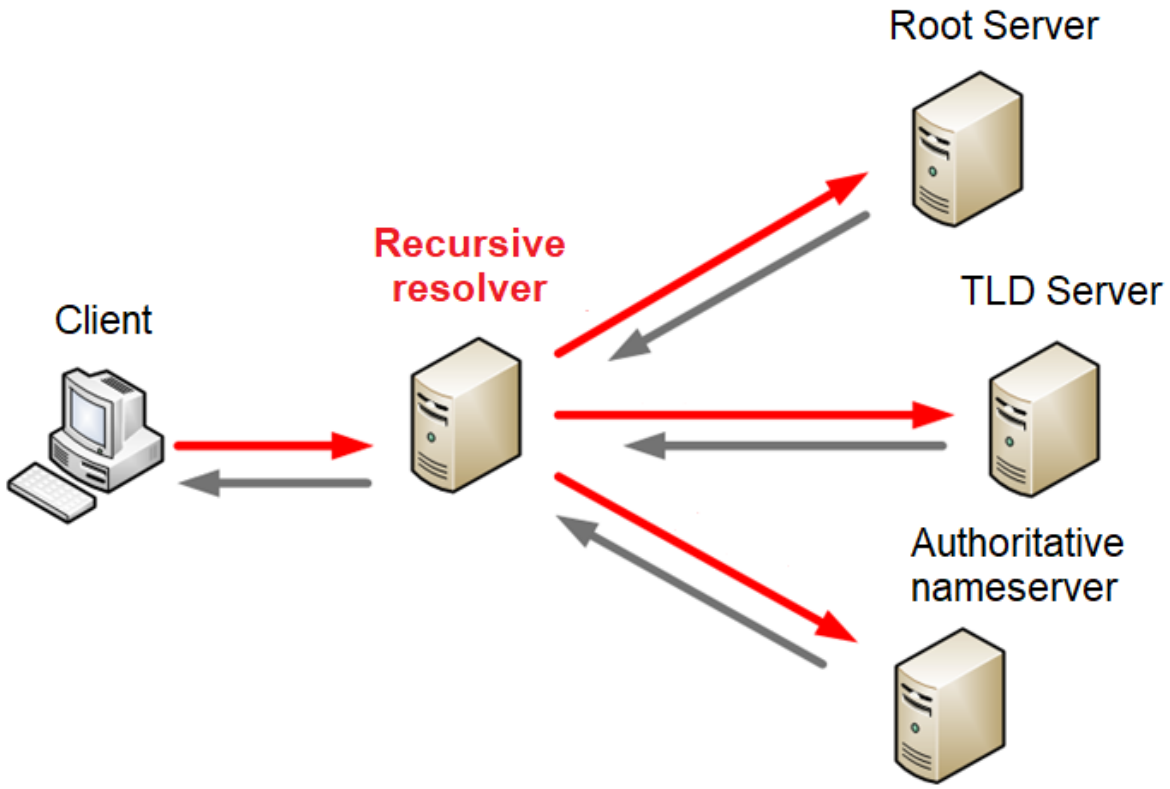
DNS Server Types

- Recursive resolver
- Root nameserver
- TLD nameserver (top-level domain)
- Authoritative nameserver



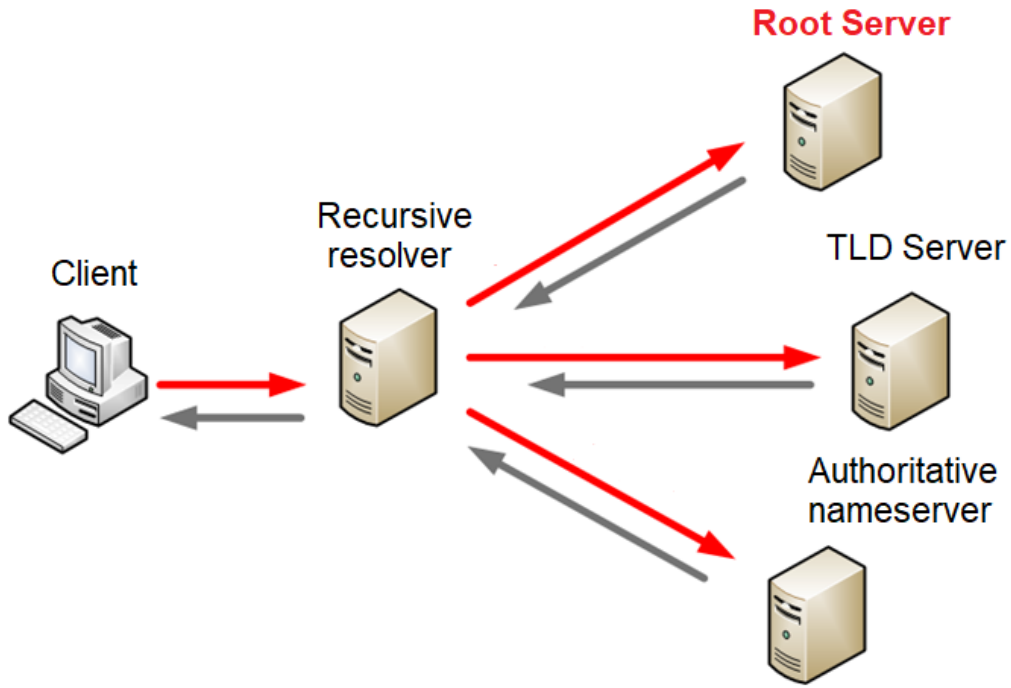
Recursive Resolver

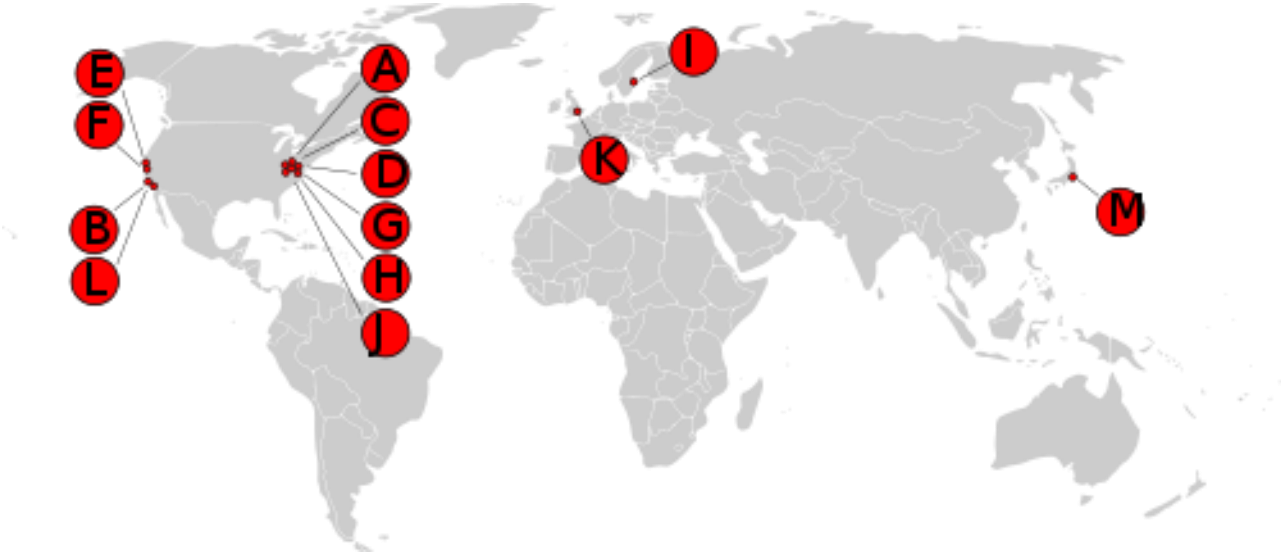
- A recursive resolver (also known as a DNS recursor) is the first step in a DNS query.
- The recursive resolver acts as a **middleman** between a client and a DNS nameserver.
- After receiving a DNS query from a web client, a recursive resolver will either respond with cached data, or send a request to a root nameserver, followed by another request to a TLD nameserver, and then one last request to an authoritative nameserver.
- After receiving a response from the authoritative nameserver containing the requested IP address, the recursive resolver then sends a response to the client.



Root nameserver

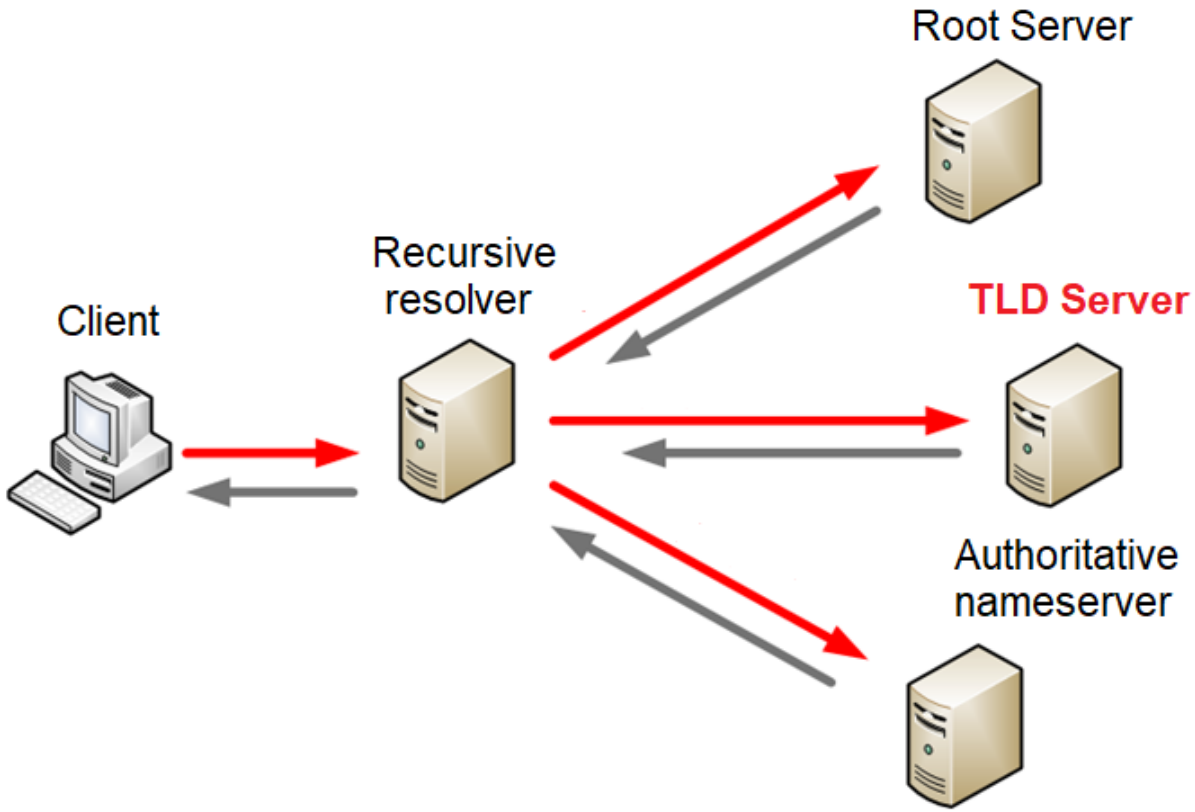
- The 13 DNS root nameservers are known to every recursive resolver, and they are the first step in a recursive resolver's quest for DNS records.
- A root server accepts a recursive resolver's query which includes a domain name, and the root nameserver responds by directing the recursive resolver to a TLD nameserver, based on the extension of that domain (.com, .net, .org, etc.).
- The root nameservers are overseen by a nonprofit called the Internet Corporation for Assigned Names and Numbers (ICANN).
- https://root-servers.org/





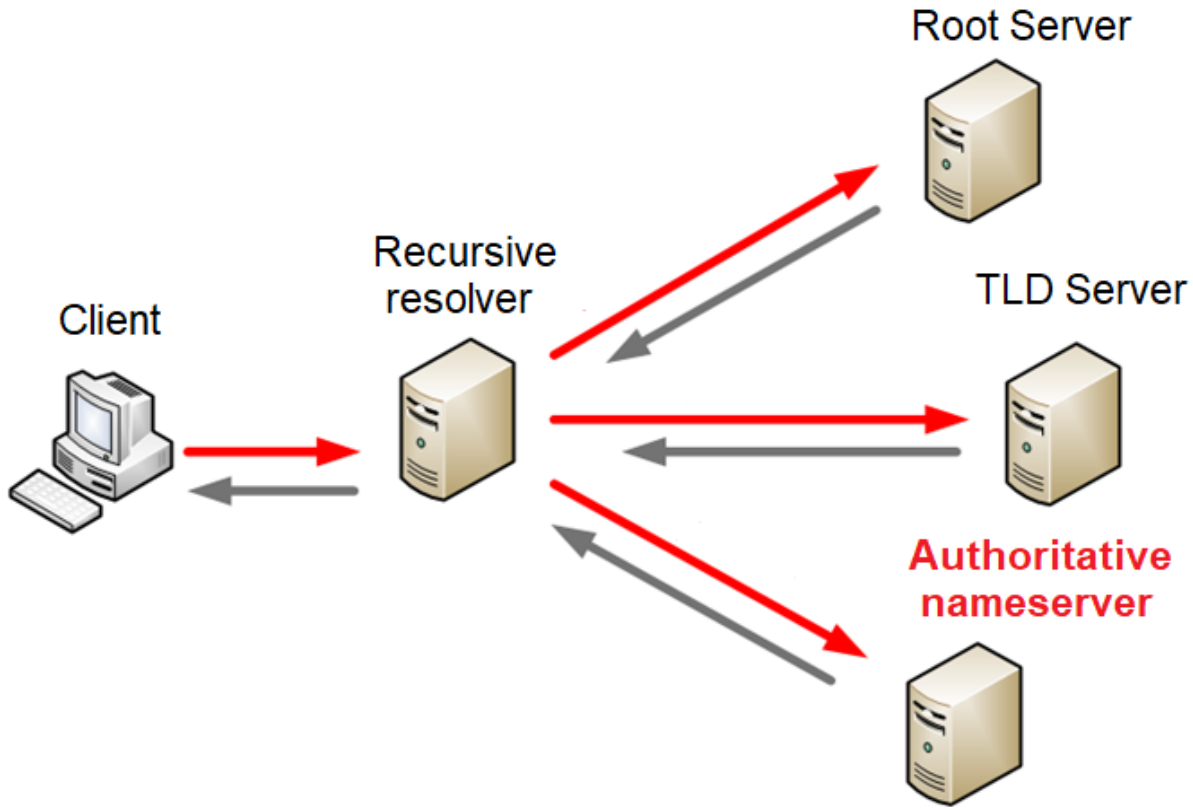
Top-level domain Server

- A TLD nameserver maintains information for all the domain names that share a common domain extension, such as .com, .net, or whatever comes after the last dot in a url.
- Management of TLD nameservers is handled by the Internet Assigned Numbers Authority (IANA), which is a branch of ICANN. The IANA breaks up the TLD servers into two main groups:
  - **Generic top-level domains**: These are domains that are not country specific, some of the best-known generic TLDs include .com, .org, .net, .edu, and .gov.
  - **Country code top-level domains**: These include any domains that are specific to a country or state. Examples include .uk, .us, .ua, and .jp.



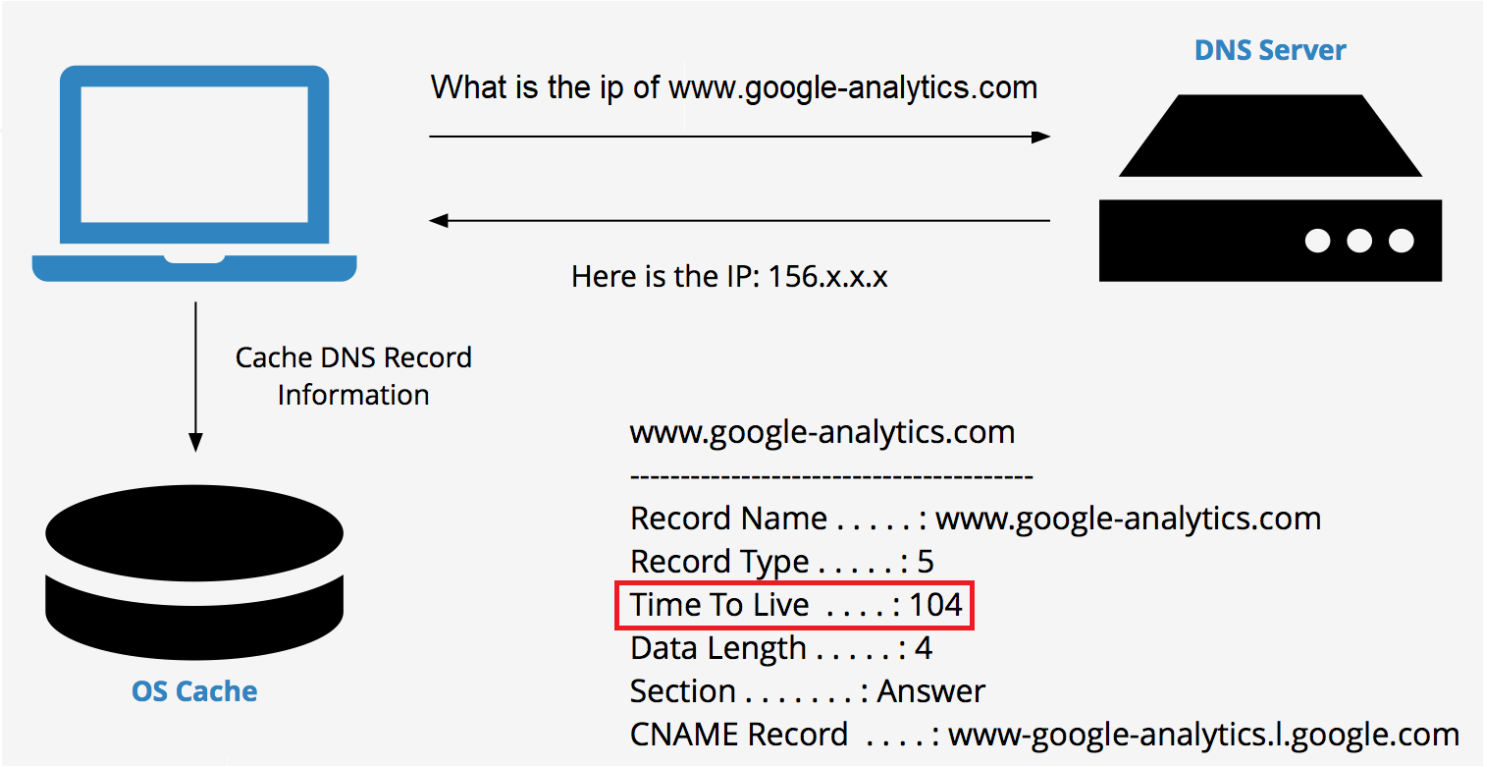
Authoritative nameserver

- The authoritative nameserver is usually the resolver's last step in the journey for an IP address.
- The authoritative nameserver **contains information specific to the domain name it serves,** for example epam.com and it can provide a recursive resolver with the IP address of that server found in the DNS A record.



DNS cache

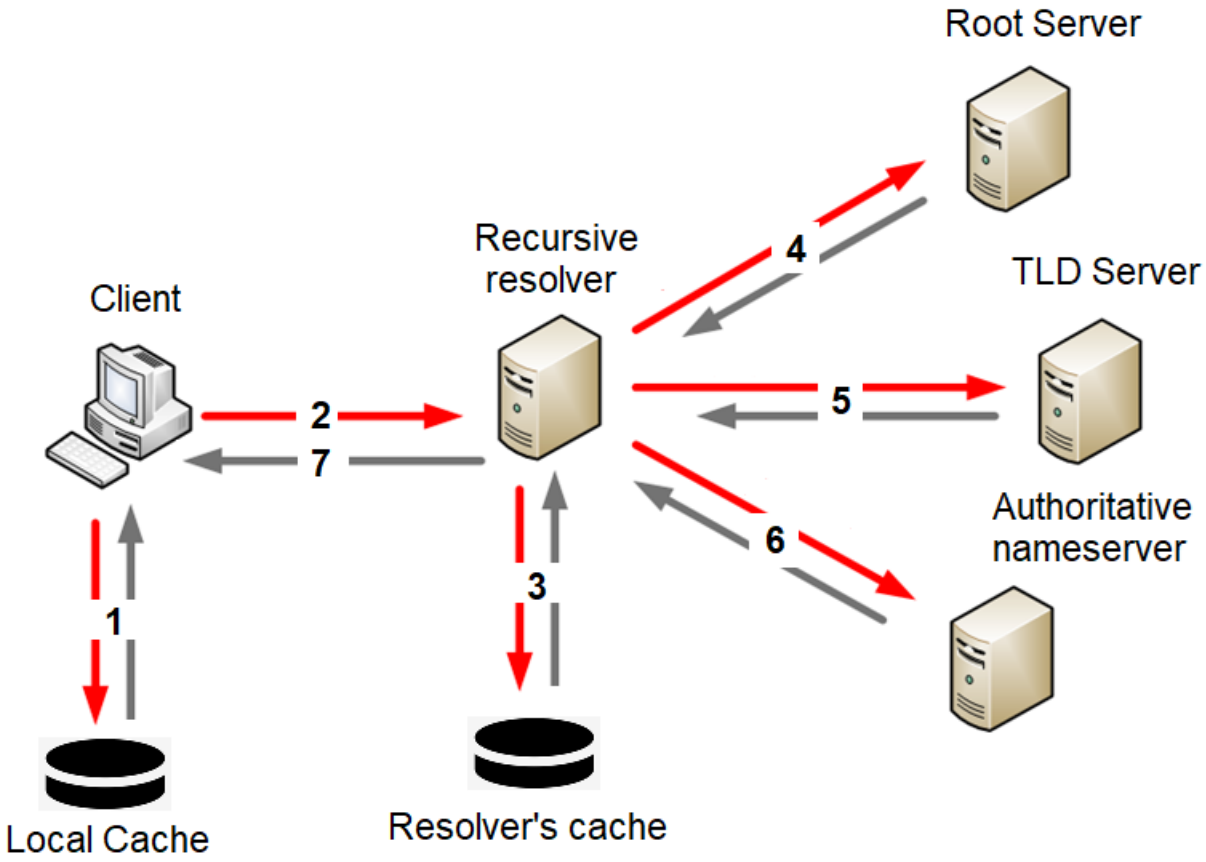
- A DNS cache (sometimes called a DNS resolver cache) is a temporary database, maintained by a computer's operating system, that contains records of all the recent visits and attempted visits to websites and other internet domains.
- TTL (time to live), is a commonly used setting for defining how long a DNS record should remain in a DNS resolver's cache. Using TTL helps improve website speed since if the DNS lookup is already cached locally, it can be retrieved much faster than if a DNS server is required to complete the full lookup process.



- Caching DNS records is very beneficial in terms of improving speeds as well as the reducing the amount of load DNS resolvers around the globe experience.
- Setting TTL too high can cause issues. For instance, if a change to a DNS record must be made, you'll need to wait for the TTL to expire before the change will take effect.

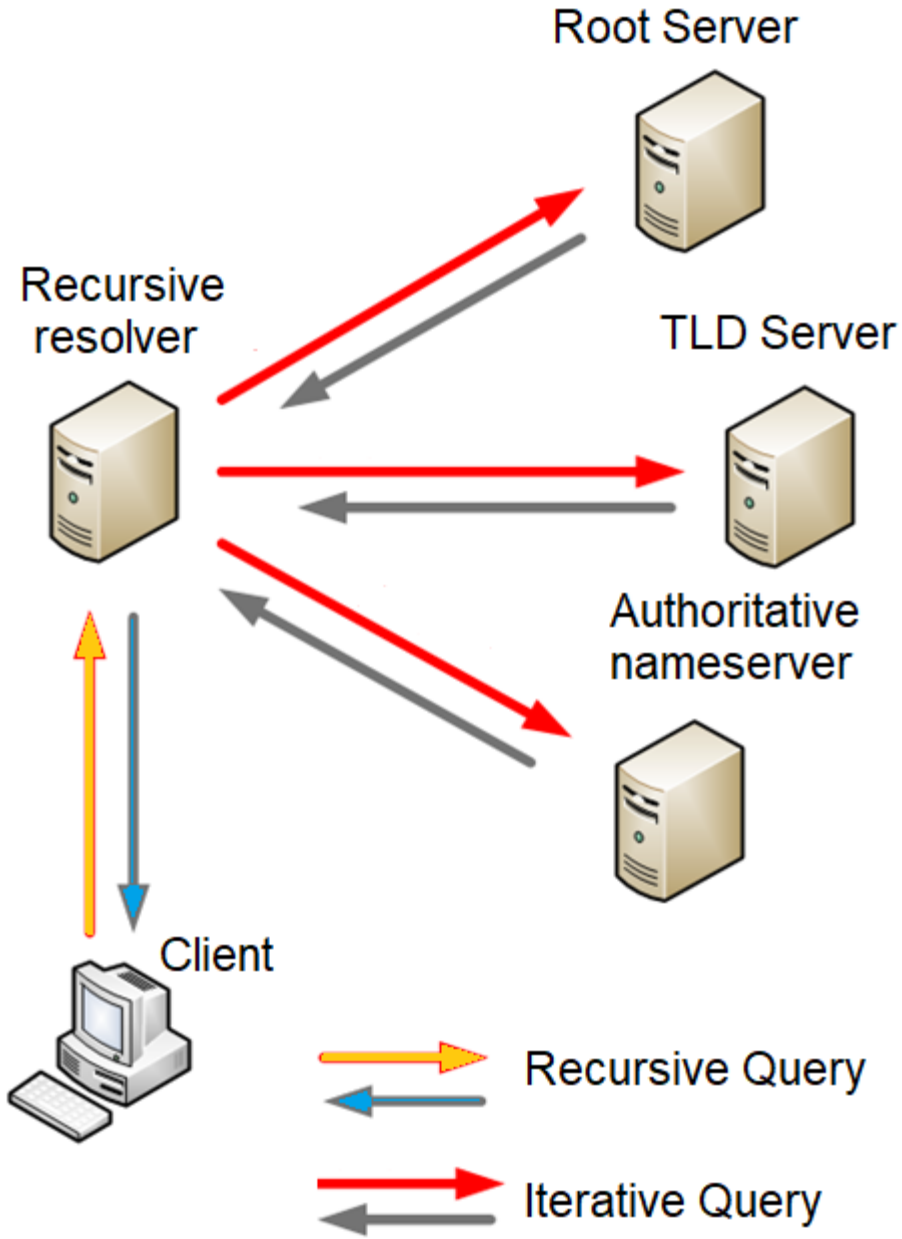
DNS server lookup process

1. Client asks local cache
2. Client asks recursive resolver
3. Resolver asks personal cache
4. Resolver asks root server
5. Resolver asks TLD server
6. Resolver asks authoritative name server
7. Resolver answers to client



DNS resolving – request types

- In **Recursive name query**, the DNS client requires that the DNS server respond to the client with either the requested resource record or an error message if the record or domain name doesn't exist. If DNS server is not able to resolve the requested query, then it forwards the query to another DNS server until it gets an answer, or the query fails.
- An **Iterative name query** is one in which a DNS client allows the DNS server to return the best answer it can give based on its cache or zone data. If the queried DNS server does not have an exact match for the queried name, the best possible information it can return is a referral. The DNS client can then query the DNS server for which it obtained a referral. It continues this process until it locates a DNS server that is authoritative for the queried name, or until an error or time-out condition is met.



DNS Records

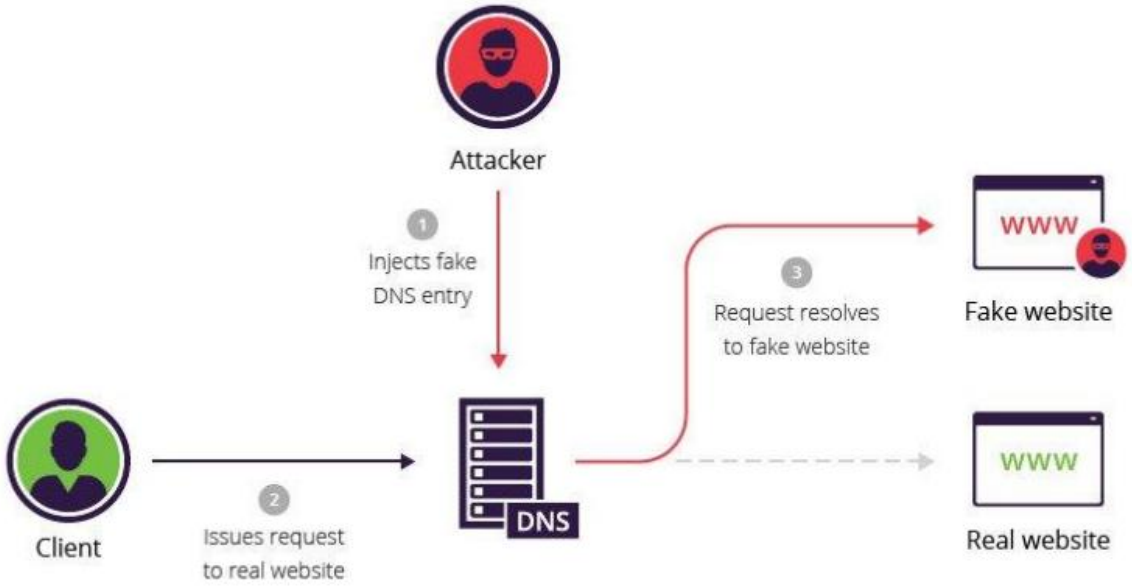
- DNS server stores different types of resource records used to resolve names
- Any record contain the **name**, **address**, and **type**
- Some record types:
  - **A** - an end device address
  - **NS** - an authoritative name server
  - **CNAME** - the canonical name for an alias; used when multiple services have the single network address but each service has its own entry in DNS
  - **MX** - mail exchange record; maps a domain name to a list of mail exchange servers
  - **PTR** - used as "reverse records" - to map IP addresses to domain names

Common DNS Record Types	
Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

DNS security

- The **DNS Security Extensions** (DNSSEC) strengthens authentication in DNS using digital signatures based on public key cryptography.
- With DNSSEC, it's not DNS queries and responses themselves that are cryptographically signed, but rather DNS data itself is signed by the owner of the data.
- Every DNS zone has a public/private key pair. The zone owner uses the zone's private key to sign DNS data in the zone and generate digital signatures over that data.

DNS cache poisoning attack



- The zone's public key is published in the zone itself for anyone to retrieve. Any recursive resolver that looks up data in the zone also retrieves the zone's public key, which it uses to validate the authenticity of the DNS data.
- The resolver confirms that the digital signature over the DNS data it retrieved is valid. If so, the DNS data is legitimate and is returned to the user. If the signature does not validate, the resolver assumes an attack, discards the data, and returns an error to the user.

Summary

- The Domain Name System (DNS) is the hierarchical naming system used to identify computers reachable through the Internet.
- The resource records contained in the DNS associate domain names with other forms of information. These are most commonly used to map domain names to the numerical IP addresses computers.
- DNS is based on groups of different types of DNS servers that are used in the address resolution process.
- DNS can pose a security risk via DNS cache poisoning and many other attacks, then security measures need to be taken.