CC5303 – Sistemas Distribuidos

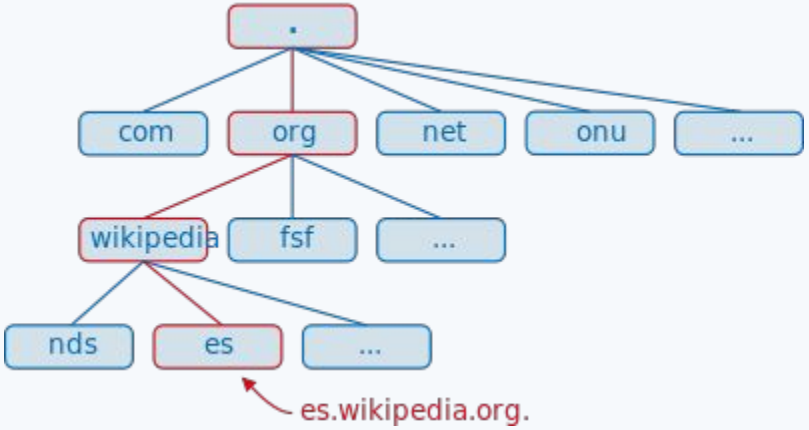
2.- Naming

Parte 2

Sebastián Blasco V.

DNS

- El espacio de nombre DNS está organizado jerárquicamente como las raíces de un árbol de nombres estructurados.



DNS

Tipo	Entidad asociada	Descripción
SOA	Zone	Contiene información de la zona representada, su administrador, el host donde se encuentra la raíz de esa zona, etc.
A	Host	Contiene la IP del nodo a quien representa, en caso de múltiples IP, se utilizarán múltiples registros A
MX	Domain	Referencia al mailserver del dominio (quien procesará todo el correo para un dominio determinado)
SRV	Domain	Nombre del servidor para un servicio específico (ejemplo: Web)
NS	Zone	El nombre del NameServer que implementa una zona específica
CNAME	Node	*Canonical Name*. Nombre primario de un nodo. Link simbólico.
PTR	Host	Contiene el nombre primario de un host para consultas por IP. Por ejemplo: dichato.dcc.uchile.cl es 192.80.24.4, por lo tanto PTR sería 4.24.80.192.in-addr.arpa
HINFO	Host	Información adicional del host
TXT	Any kind	Información adicional de la entidad representada por el nodo

DNS

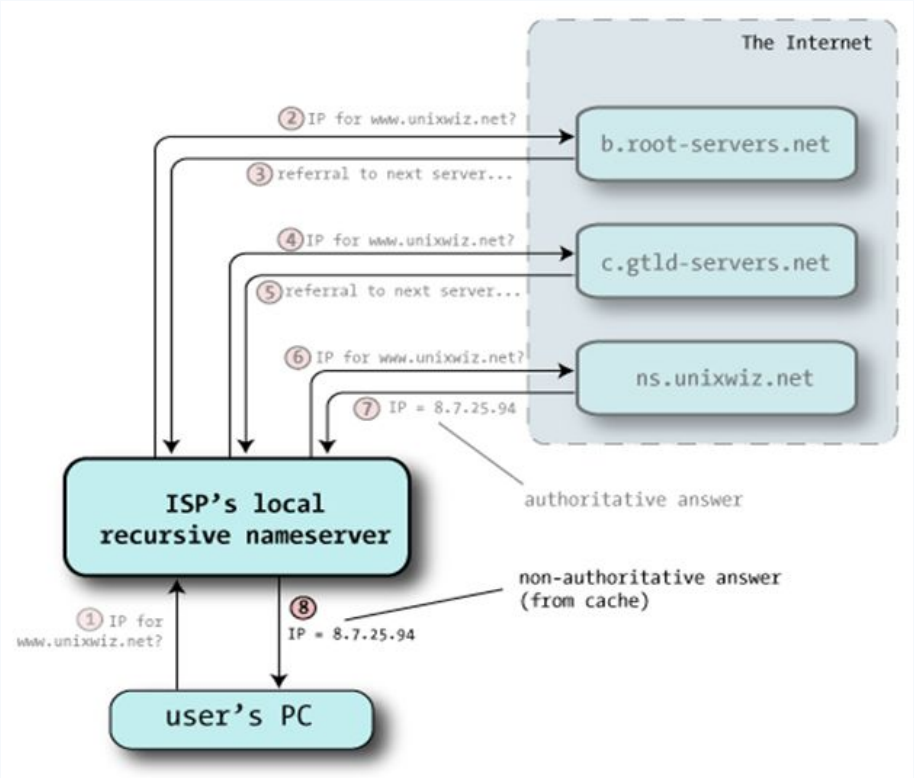
Ejemplo archivo de Zona

```
$ORIGIN example.com.
$TTL 86400
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.example.com.
      IN     NS     dns2.example.com.

      IN     MX     10     mail.example.com.
      IN     MX     20     mail2.example.com.

             IN     A       10.0.1.5

server1      IN     A       10.0.1.5
server2      IN     A       10.0.1.7
dns1         IN     A       10.0.1.2
dns2         IN     A       10.0.1.3

ftp          IN     CNAME   server1
mail         IN     CNAME   server1
mail2        IN     CNAME   server2
www          IN     CNAME   server2
```

DNS

Consulta general

- Cliente pregunta recursivamente
- El ISP pregunta iterativamente



DNS

dcc.uchile.cl@8.8.8.8 (Google):

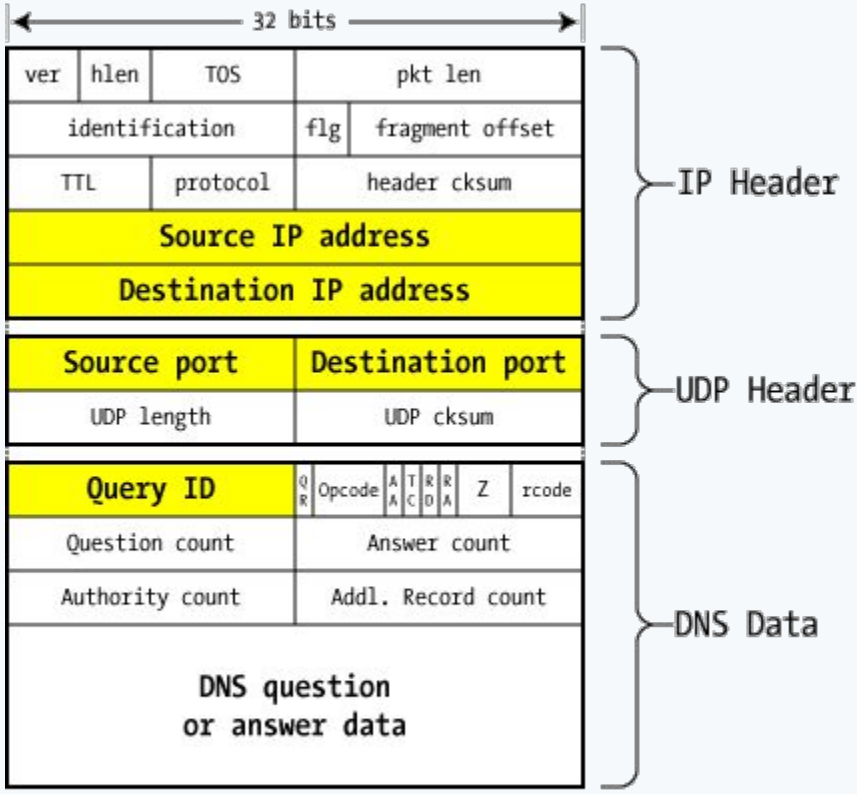
dig +noadditional +noquestion +nocomments +nocmd +nostats +trace dcc.uchile.cl. @8.8.8.8

```
.                       5429    IN      NS      m.root-servers.net.
.                       5429    IN      NS      k.root-servers.net.
.                       5429    IN      NS      h.root-servers.net.
.                       5429    IN      NS      l.root-servers.net.
.                       5429    IN      NS      i.root-servers.net.
.                       5429    IN      NS      j.root-servers.net.
.                       5429    IN      NS      d.root-servers.net.
.                       5429    IN      NS      a.root-servers.net.
.                       5429    IN      NS      b.root-servers.net.
.                       5429    IN      NS      c.root-servers.net.
.                       5429    IN      NS      e.root-servers.net.
.                       5429    IN      NS      f.root-servers.net.
.                       5429    IN      NS      g.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 36 ms

cl.                     172800  IN      NS      a.nic.cl.
cl.                     172800  IN      NS      b.nic.cl.
cl.                     172800  IN      NS      c.nic.cl.
cl.                     172800  IN      NS      cl1.dnsnode.net.
cl.                     172800  IN      NS      cl-ns.anycast.pch.net.
cl.                     172800  IN      NS      sns-pb.isc.org.
;; Received 408 bytes from 193.0.14.129#53(193.0.14.129) in 46 ms

uchile.cl.              3600    IN      NS      ns2.uchile.cl.
uchile.cl.              3600    IN      NS      ns4.uchile.cl.
uchile.cl.              3600    IN      NS      ns1.uchile.cl.
;; Received 133 bytes from 200.7.4.7#53(200.7.4.7) in 63 ms

dcc.uchile.cl.          10800   IN      NS      ns1.dcc.uchile.cl.
dcc.uchile.cl.          10800   IN      NS      ns2.uchile.cl.
dcc.uchile.cl.          10800   IN      NS      ns.dcc.uchile.cl.
;; Received 132 bytes from 146.83.185.209#53(146.83.185.209) in 159 ms

dcc.uchile.cl.          21600   IN      A       192.80.24.4
dcc.uchile.cl.          21600   IN      NS      ns2.dcc.uchile.cl.
dcc.uchile.cl.          21600   IN      NS      ns2.uchile.cl.
dcc.uchile.cl.          21600   IN      NS      ns.dcc.uchile.cl.
dcc.uchile.cl.          21600   IN      NS      ns1.dcc.uchile.cl.
;; Received 166 bytes from 192.80.24.2#53(192.80.24.2) in 162 ms
```

DNS

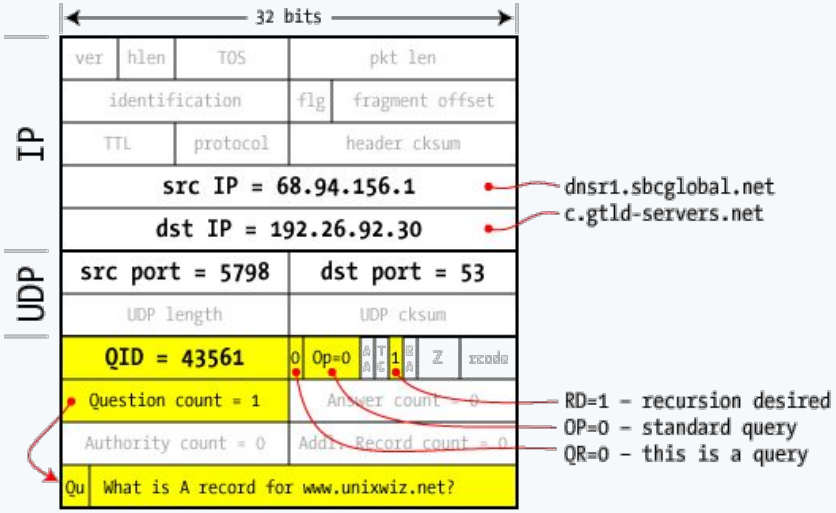
Estructura paquete DNS

- QueryID: #query
- QR: 0 Query / 1 Response
- QPCODE: 0 para Queries Standard
- AA: Respuesta Autoritativa
- TC: Truncado, si no cabe en 1 solo paquete
- RD: Recursion Desired
- RA: Recursion Available
- Z: zeros… 0
- rcode: Código de respuesta, success o failure
- Question/Answer/Authority/Aditional count:
  Indica número de elementos de dicho tipo enviados



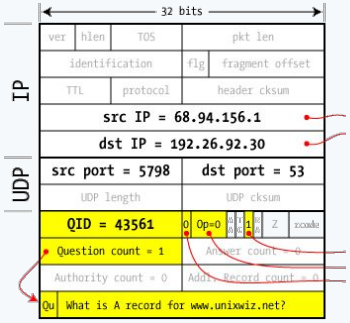
DNS

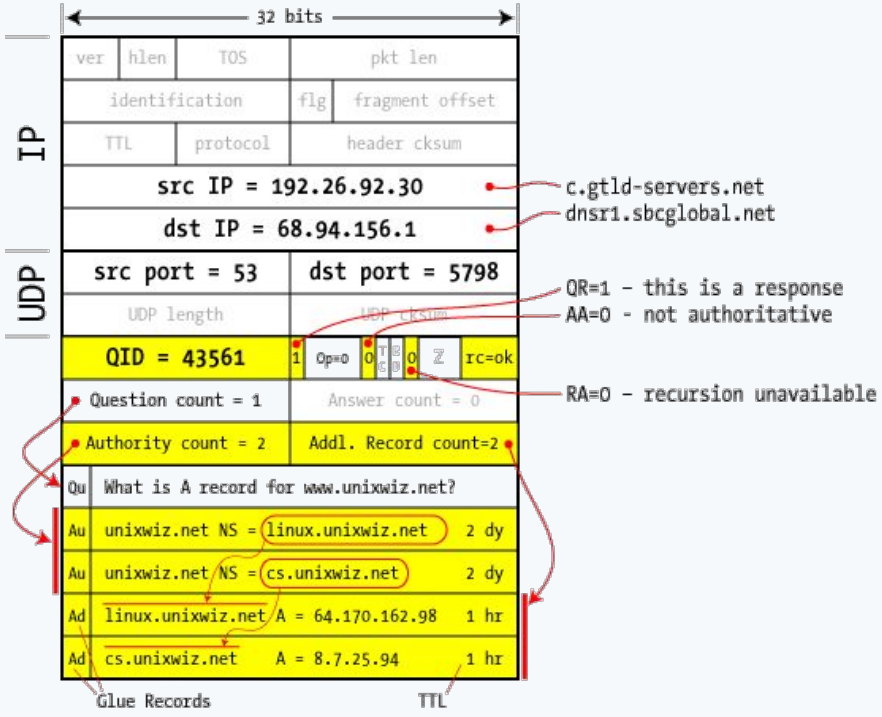
Dinámica DNS



DNS

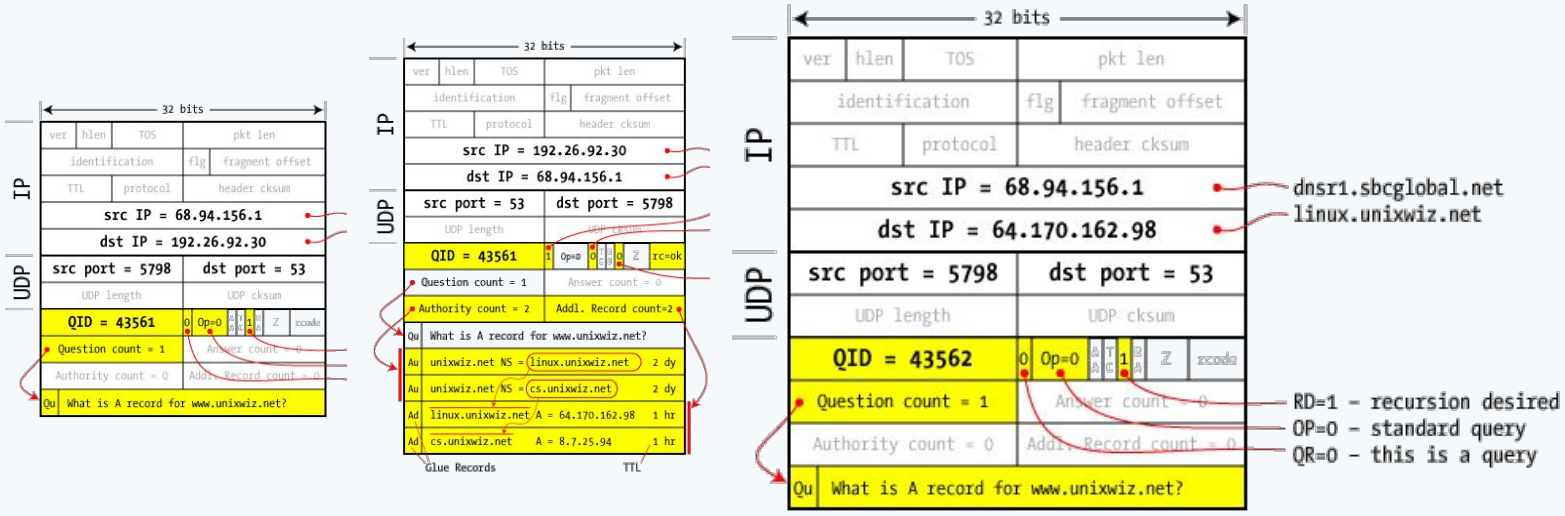
Dinámica DNS





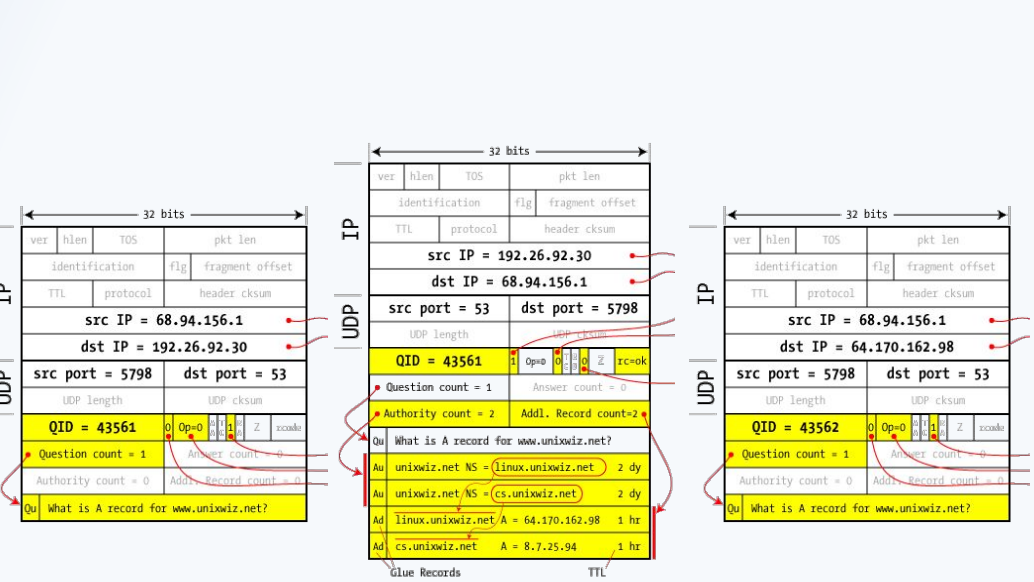
DNS

Dinámica DNS



DNS

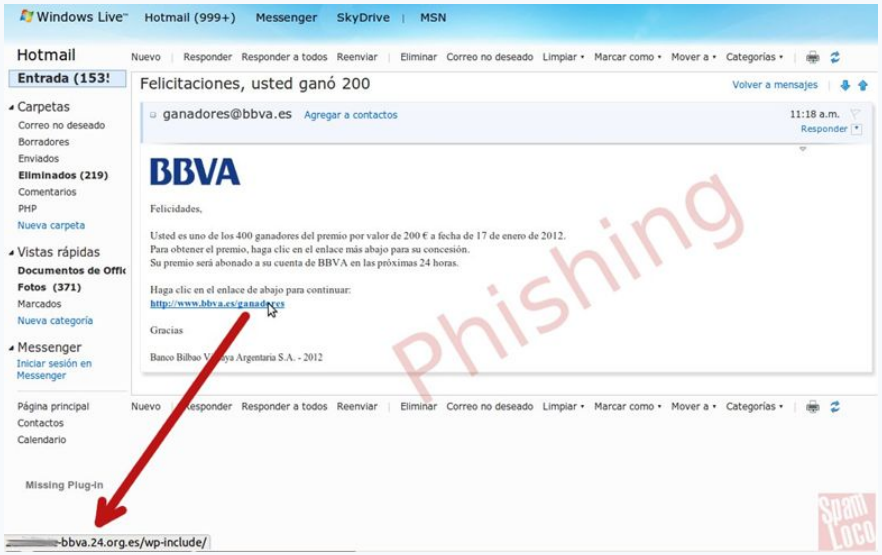
Dinámica DNS

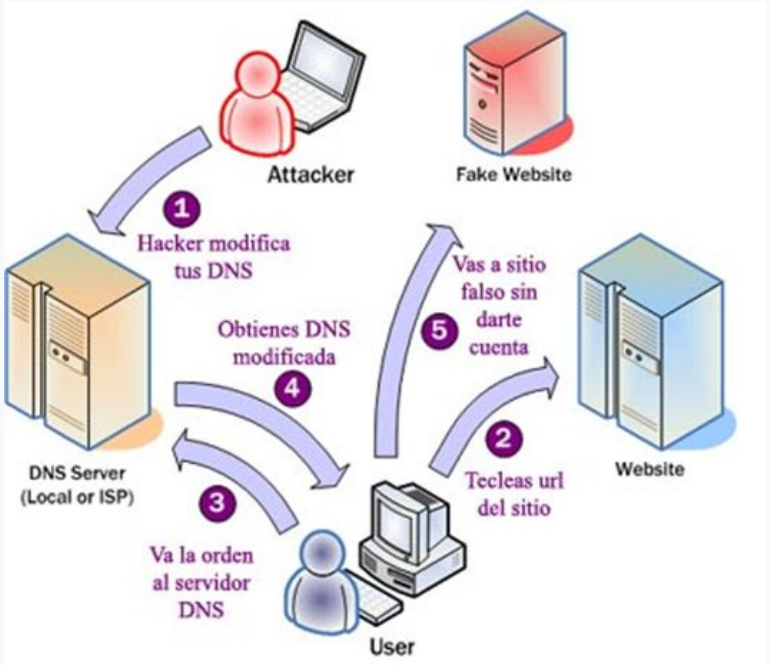


DNS

Problemas DNS

- El envenenamiento DNS es uno de los problemas más importantes en Internet.
- No es como el phishing… es mucho más grave!

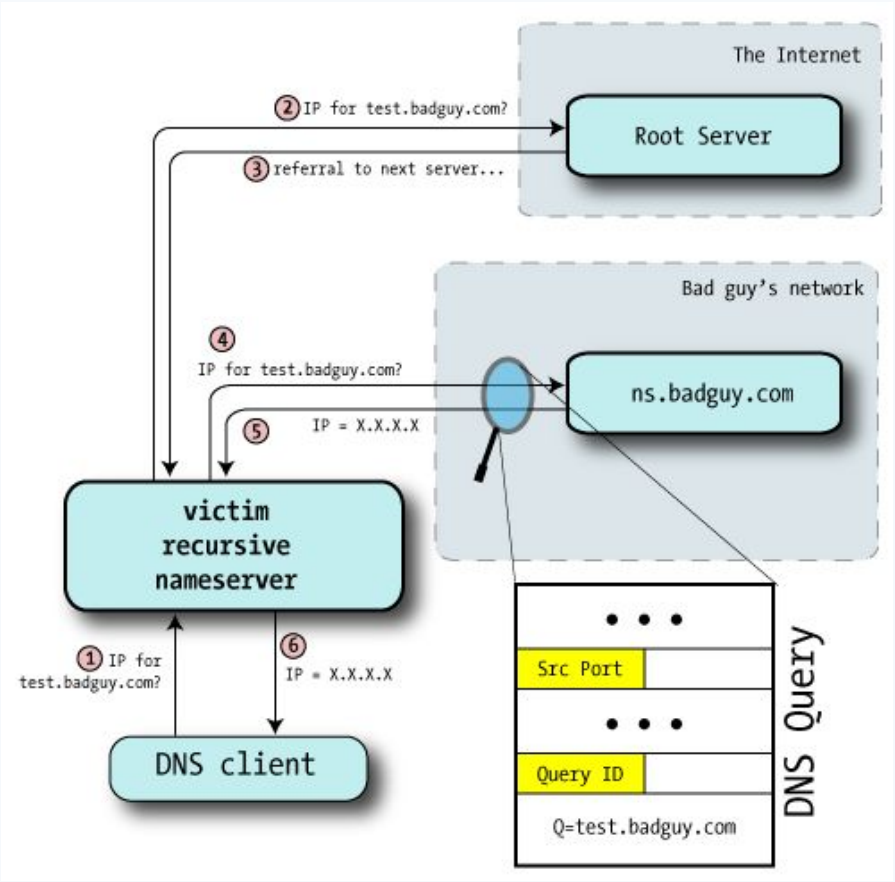




DNS

Problemas DNS: DNS Poisoning

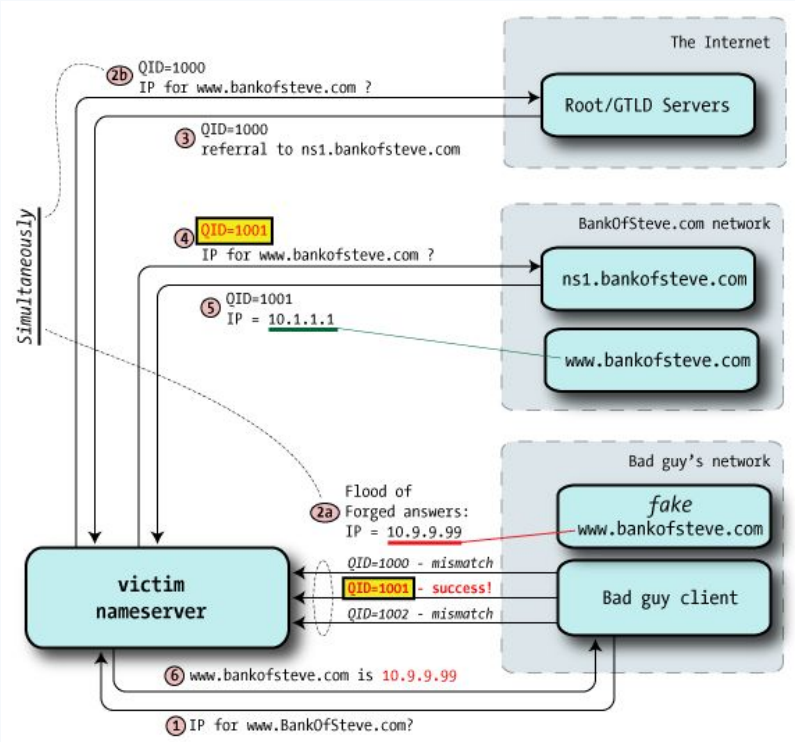
- Adivinando QueryID
  - Al final de este proceso se obtiene:
    - QueryID Actual
    - Puerto de comm.
  - Hasta aquí no se ha envenenado nada… (aún)



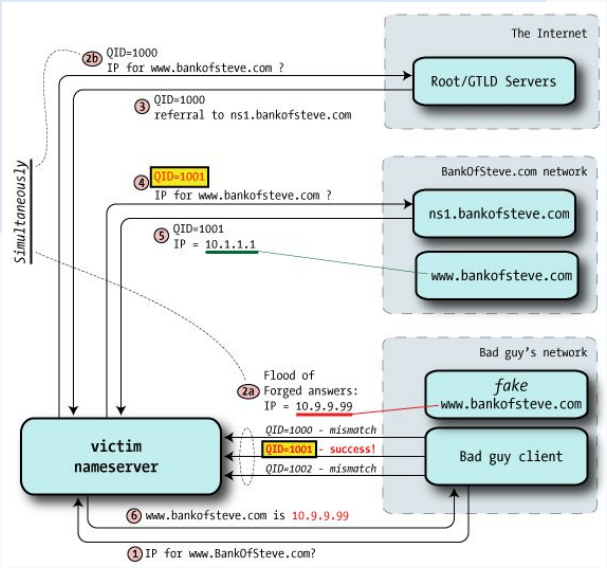
DNS

Problemas DNS: DNS Poisoning

- Envenenando por el principio DNS
  - “La primera respuesta buena sirve!”.



DNS



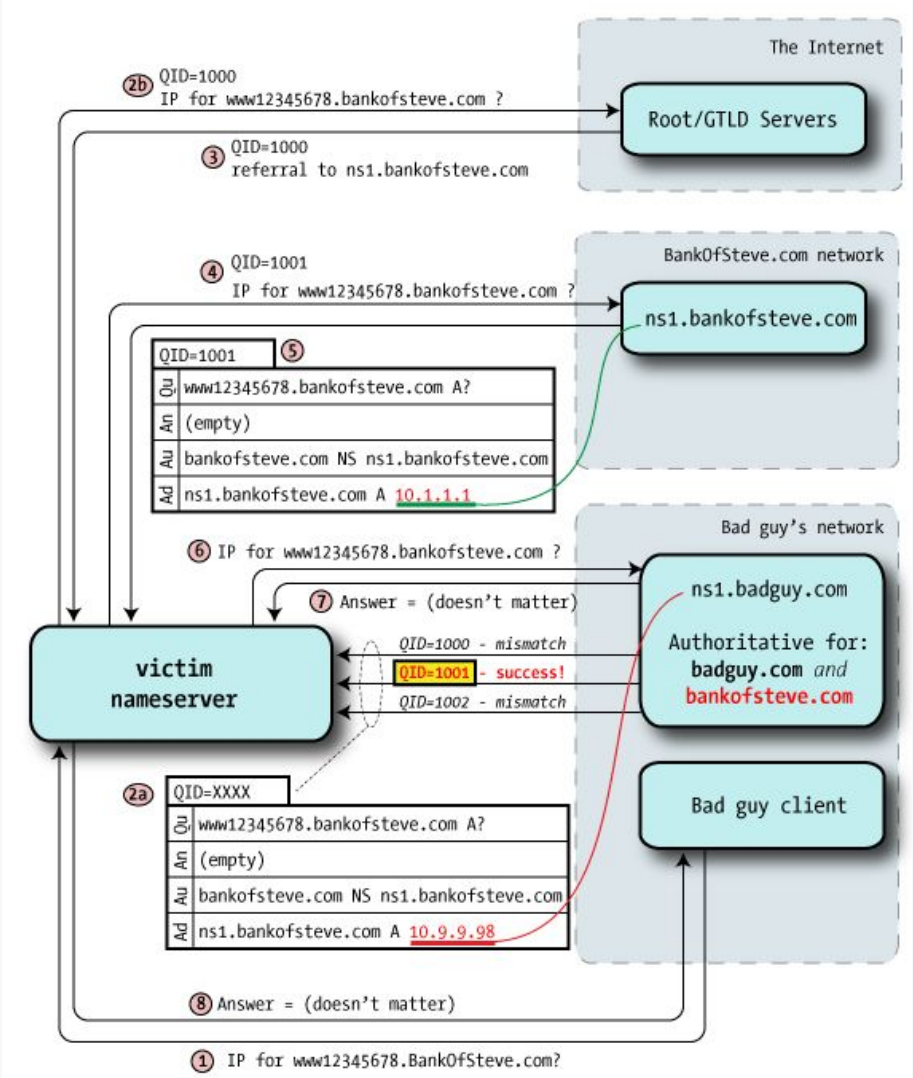
Problemas DNS: DNS Poisoning

- Envenenando por el principio DNS
  - Consideraciones:
    - Atacante debe poder adivinar el QID
    - El registro a envenenar no debe estar en caché
    - Atacante debe ser más veloz que el servidor real.
  - Efecto:
    - Se ha cambiado la ip de respuesta de un registro en particular.
  - Mitigaciones:
    - Randomizar QID
      - Pero... el campo QID es sólo de 16 bit ~64k posibilidades

DNS

Problemas DNS: DNS Poisoning

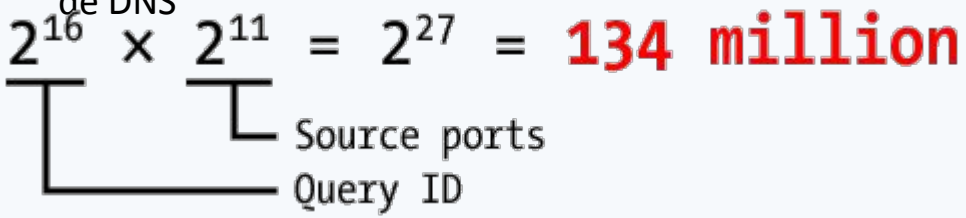
- Dan Kaminsky
  - Permite hacerse con el **envenenamiento de toda una zona completa** al intervenir con una resp. autoritativa con TTL tan duradero como quiera el atacante
  - Se ha reportado que este tipo de ataques toma alrededor de 10 segundos en adivinar el QueryID.



DNS

Problemas DNS: DNS Poisoning

- Dan Kaminsky
  - Terrible!!!
  - El problema es que los 16 bits del QID parecen no ser suficientes… Modificarlo? inviable
  - Idea
    - Aleatorizar puertos de comm.
      - ej. Microsoft habilitó 2500 puertos por defecto para la labor randomizada de DNS



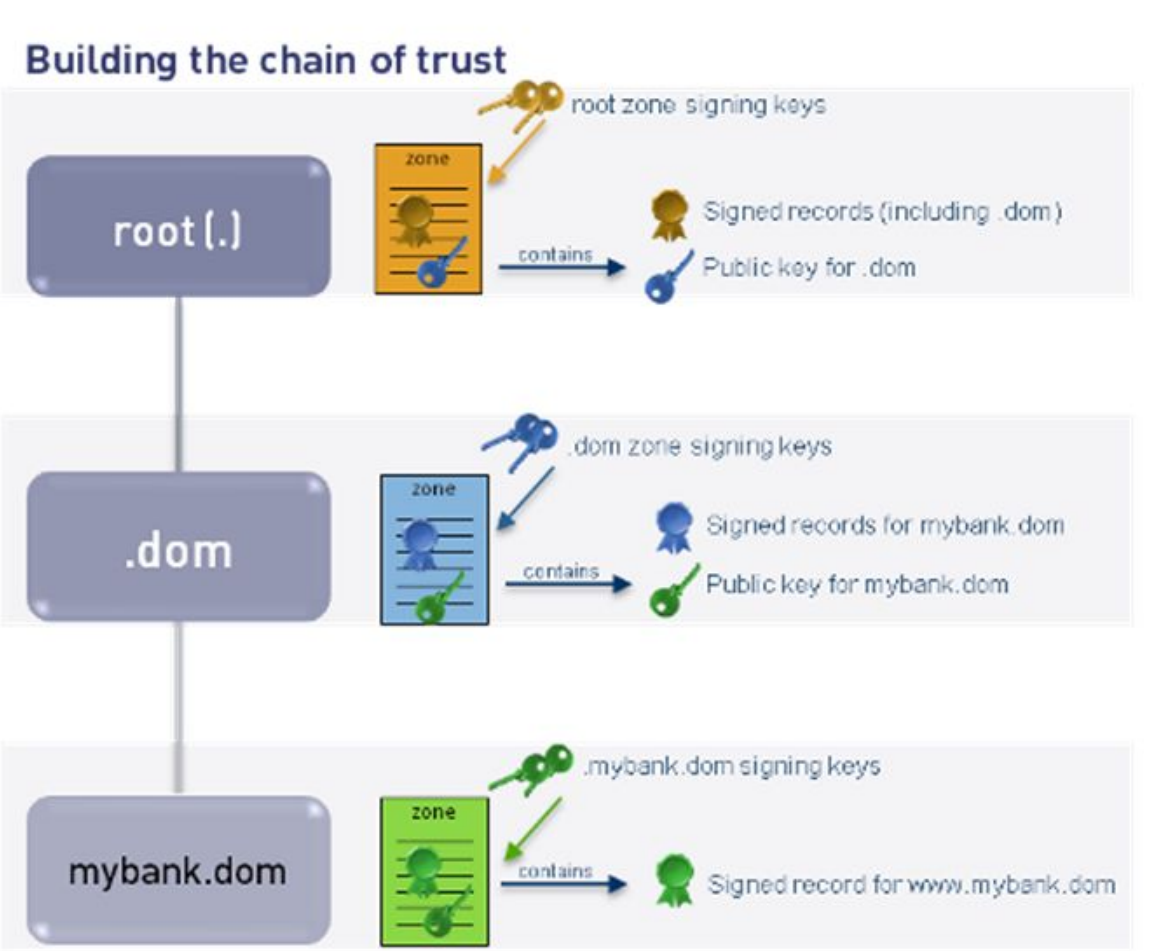
DNSSEC

Firma digital de los datos a fin de tener la seguridad de que son válidos.

Se basa en un sistema de firmado con clave público/privada y una cadena de confianza.

No cifra los datos. Tan solo certifica la validez de la dirección del sitio que se visita.

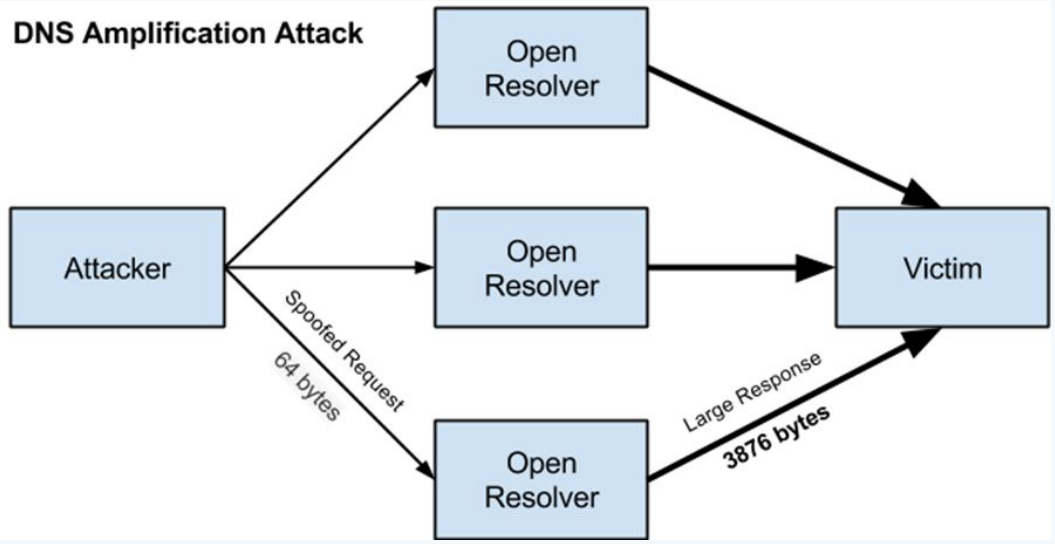
DNSSEC


Building the chain of trust
root zone signing keys
zone
root (.)
contains
Signed records (including .dom)
Public key for .dom
.dom zone signing keys
zone
.dom
contains
Signed records for mybank.dom
Public key for mybank.dom
.mybank.dom signing keys
zone
mybank.dom
contains
Signed record for www.mybank.dom

DNSSEC

Dificultades?

- Para que DNSSEC tenga sentido, debe ser implementado íntegramente por los niveles de dominios.
- Comunicación más pesada



Tipos de nombres

La pregunta clave es:

¿Cómo resolver nombres e identificadores de direcciones?

Existen distintas maneras de implementar nombres en un sistema de naming:

- Nombres planos
- Nombres estructurados
- **Nombres basados en atributos**

Nombres basados en Atributos

- Es muy importante tener la mayor información disponible para realizar una búsqueda efectiva de entidades. Este método requiere del usuario que pueda proporcionar una descripción simple de lo que busca.

- Describir a una entidad en términos de pares:
  - *<atributo, valor>*

- Ej. un sistema de correo electrónico
  - *<remitente, correo>*
  - *<destinatario, correo>*
  - *<asunto, correo>*

Nombres basados en Atributos

- RDF (Resource Description Framework)
  - Modelo de datos para metadatos.
  - Método general para la descripción conceptual o modelado de la información
  - Los recursos se describen como tríos que constan de un sujeto, un predicado, y un objeto.
    - Ej. *(Persona, nombre, Alice)* describe un recurso **Persona** cuyo **nombre** es **Alice**. En RDF, cada sujeto, predicado y objeto puede ser un recurso por sí mismo
    - Ej

<http://en.wikipedia.org/Tony_Benn> <http://purl.org/dc/elements/1.1/title> "Tony Benn" .
<http://en.wikipedia.org/Tony_Benn> <http://purl.org/dc/elements/1.1/publisher> "Wikipedia" .

Nombres basados en Atributos

- RDF (Resource Description Framework)
  - A diferencia de los sistemas de nombre estructurados, buscar valores en un sistema de nombre basados en atributos básicamente requiere una **búsqueda exhaustiva** a través de todos los descriptores.
  - Uso de RDF no tuvo el auge esperado :(