****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**0 – Introdução Protocolo DNS**

A Internet utiliza endereços IP para identificar uma entidade de rede, porém nós preferimos utilizar nomes em vez de números. Que mais fácil de guardar (OK. Sei que isso não é verdade para algumas pessoas =).

Para isso necessitamos de um serviço que faça a resolução de nome para IP, e de IP para nome. Assim nasceu o host file, um arquivo que continha o mapeamento de nome para IP e vice-versa.

Enquanto a Internet era pequena o host file atendeu bem, já que, existia um host file master onde era acrescentado todas as entidades que entrava na rede e depois este arquivo era compartilhado para todos os outros hosts.

Nos dias de hoje isso seria inviável com o número crescente de dispositivos conectados na Internet. Teríamos dois problemas o crescimento deste arquivo seria absurdo e o tráfego gerado para atualizar todos os hosts file inviabilizaria a Internet como a conhecemos.

Uma solução seria descentralizar essas informações, dividindo elas em pequenas informações e distribuí-las entre computadores espalhados pelo mundo. Assim em vez de mapeamos todos os hosts, nós apenas solicitamos a resolução de nome para o computador mais próximo que tenha essa função. Assim foi criado o modelo que conhecemos hoje o **DNS (Domain Name System)**.

**1 – Características do Protocolo DNS**

**1.1 – Espaços de Nomes**

Para evitar ambiguidade, os nomes das máquinas devem ser únicos, assim como os endereços IP devem ser únicos.

Um espaço de nome que mapeia cada nome para um endereço IP pode ser organizado de dois modos: **Plano** ou **Hierárquico**.

**1.1.1 – Espaço de Nome Plano**

Em um espaço de nomes um nome é atribuído a um endereço IP, este nome é uma sequência de caracteres sem nenhuma estrutura. A principal desvantagem do espaço de nome plano é a centralização dos nomes, inviabilizando seu uso em redes grade como a Internet.

**1.1.2 – Espaços de Nome Hierárquico**

Em um espaço de nome hierárquico, todo o nome é dividido em várias partes. Onde a primeira parte pode definir a natureza da organização, a segunda pode definir o nome, a terceira o departamento e assim por diante.

Desta forma uma organização pode ter autoridade sobre a natureza da organização, outra pode ter autoridade sobre o nome e os departamentos e assim por diante. Com isso, não necessitamos nos preocupar em repetir nomes de hosts ou de recursos, pois as empresas de nível superior garantem que não haverá outra organização com o mesmo nome.

Por exemplo, suponha que duas pessoas e uma empresa denomine um dos computadores de **fusion**. A primeira pessoa é delegada um nome pela autoridade central (que gerencia o espaço de nomes) de **how2security.com.br**; à segunda pessoa é delegado o nome **how2attack.com.br**, e à uma terceira empresa é delegado o nome de **incident.com.br**.

Quando todos eles organizarem os nomes completos, isto é, incluindo o nome dos computadores (no caso **fusion**), o resultado final será completamente diferente:

1. **fusion.how2security.com.br**
2. **fusion.how2attack.com.br**
3. **fusion.incident.com.br**

Esses nomes são únicos e não há necessidade de ser atribuído por uma autoridade. A zona de autoridade é responsável por delegar responsabilidades administrativas sobre porções do espaço de nomes a organizações e empresas conectadas na rede.

**1.2 – Espaços de Nome de Domínio**

O espaço de nomes de domínio **(Domain Name Space)** foi desenvolvido para oferecer uma estrutura hierárquica de nomes de espaço. Neste tipo de hierarquia, os nomes são definidos numa estrutura de árvore invertida, isto é, com a raiz no topo. A árvore pode ter somente **128 níveis**: **nível 0** **(raiz)** até o **nível 127**. Considerando que a raiz no topo une toda árvore, cada nível da árvore define um nível hierárquico.

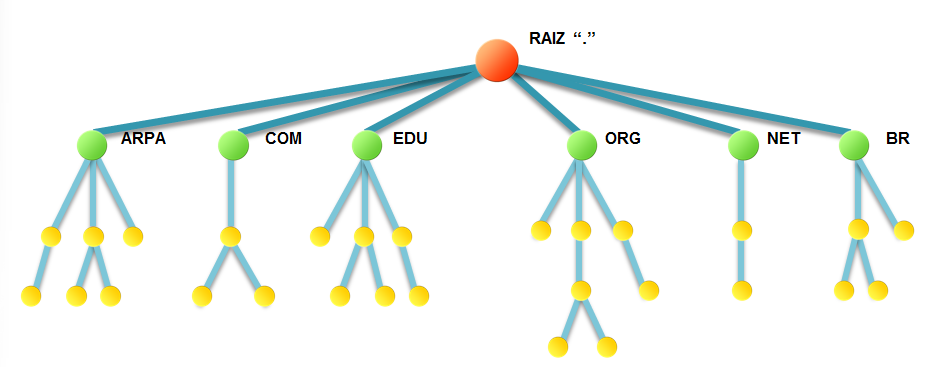


Figura 01 – Espaço de Nome de Domínio

**1.2.1 – Componentes do Nome de Nível Superior**

Cada nível da árvore possui um componente do nome, o qual é uma **string** com um máximo de **63 caracteres**. O domínio raiz da árvore tem associada uma **string nula**. O **DNS** requer que as subdivisões do espaço raiz recebam componentes do nome diferentes para assegurar a unicidade dos nomes de domínio.

**1.2.2 – Nomes de Domínios**

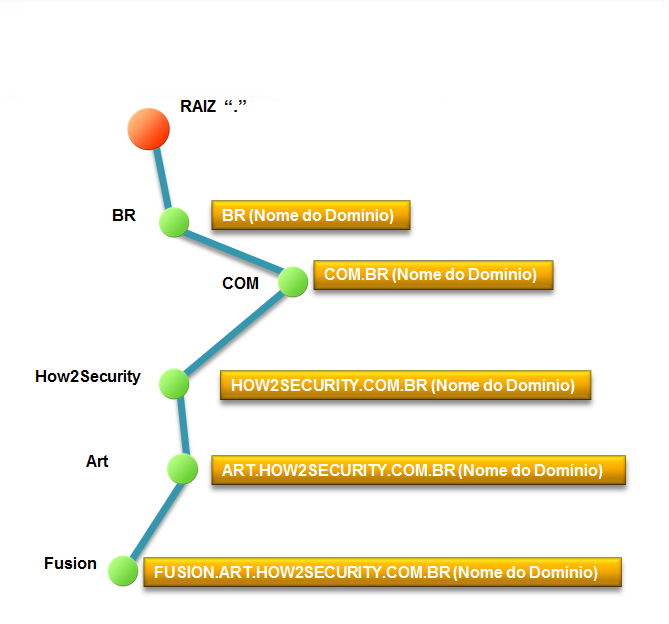
Cada nível (**nó**) na árvore possui um nome de domínio (um componente do nome). O nome de domínio completo é uma sequência de componentes do nome separados por pontos **(.)**. Os nomes do domínio são sempre lidos do nível de interesse mais baixo na direção da raiz. Isto significa que um nome de domínio completo sempre termina numa **string nula**, o que significa que o último caractere é um ponto. A Figura abaixo mostra alguns nomes de domínio. 

Figura 02 – Nomes de Domínios

* **FQDN** → Se um componente do nome termina em uma **string nula**, esse nome é denominado **FQDN (Fully Qualified Domain Name)** Um **FQDN** é um nome de domínio que contém o nome completo de um host. Ele contém todos os componentes do nome, do mais específico ao mais geral, que definem unicamente o nome do host. Por exemplo, o nome do domínio: ***fusion.art.how2security.com.br.***
* **PQDN** → Se um componente do nome não termina em uma **string nula**, esse nome é denominado **PQDN (Partial Qualified Domain Name)**. Um **PQDN** é um nome de domínio que é iniciado em certo componente de nome da hierarquia, mas não alcança a raiz. Ele é utilizado quando o nome a ser resolvido pertence ao mesmo site que o cliente. Aqui, resolver significa retirar a porção do nome, denominado sufixo, para criar um **FQDN**. Por exemplo, se um usuário no domínio **how2security.com.br** deseja obter o endereço **IP** de um computador denominado **fusion**, ele pode definir o nome parcial: **fusion.**

O cliente **DNS** adiciona o sufixo **art.how2security.com.br** antes de passar o endereço ao servidor de **DNS**. O cliente normalmente mantém uma lista de sufixo. A seguir vamos listar alguns sufixos:

* **FQDN**
  + **fusion.art.how2security.com.br**
  + **mail.how2security.com.br**
  + [**www.how2security.com.br**](http://www.how2security.com.br)
* **PQDN**
  + **fusion.art.how2security**
  + **mail.how2security**
  + **www**

**1.2.3 – Domínios**

Um domínio é uma subárvore do espaço de nomes do domínio. O nome do domínio é a coleção dos componentes de nomes até o topo da subárvore. A **Figura 03** ilustra alguns domínios. Observe que o próprio domínio pode ser dividido em domínios menores ou subdomínios, como às vezes são chamados.

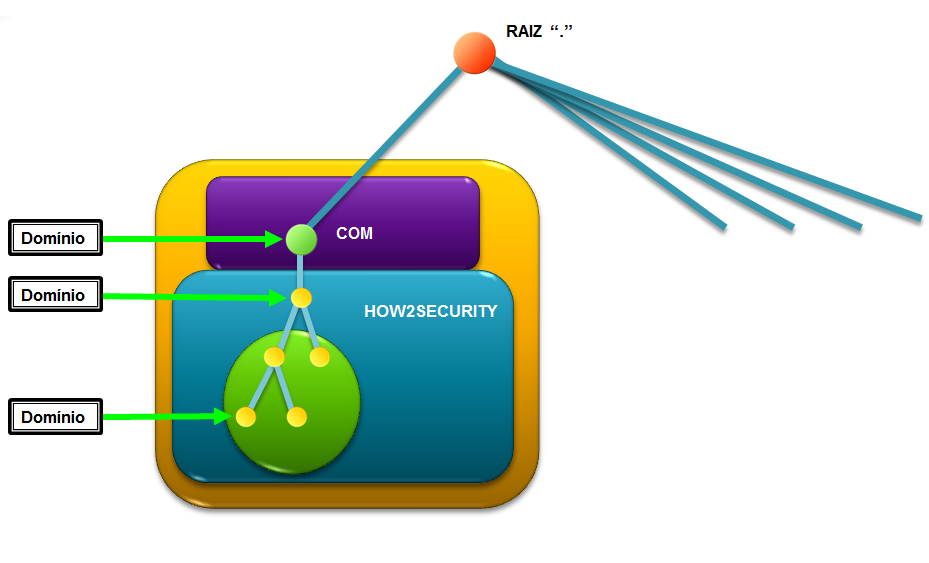


Figura 03 - Domínios

**1.3 – Distribuições do Espaço de Nomes**

A informação armazenada no espaço de nomes do domínio deve ser compartilhada, pois ela é ineficiente e pouco confiável quando fica armazenada em um computador central. Por isso, temos a hierarquia de nomes.

**1.3.1 – Hierarquia de Servidores de Nomes**

Como falamos anteriormente, o **DNS** é uma base distribuída em vários servidores. Para diminuir o tráfego, o espaço de nome é dividido em vários domínios e subdomínios, todos conectados na raiz. Assim um domínio pode crescer e ficar grande, pois cada servidor **DNS** é responsável pelo domínio e subdomínio abaixo dele, em outras palavras cada servidor **DNS** tem autoridade em seu domínio e subdomínios. Assim, é construída a hierarquia de servidores do mesmo modo que é montada a hierarquia de nomes.

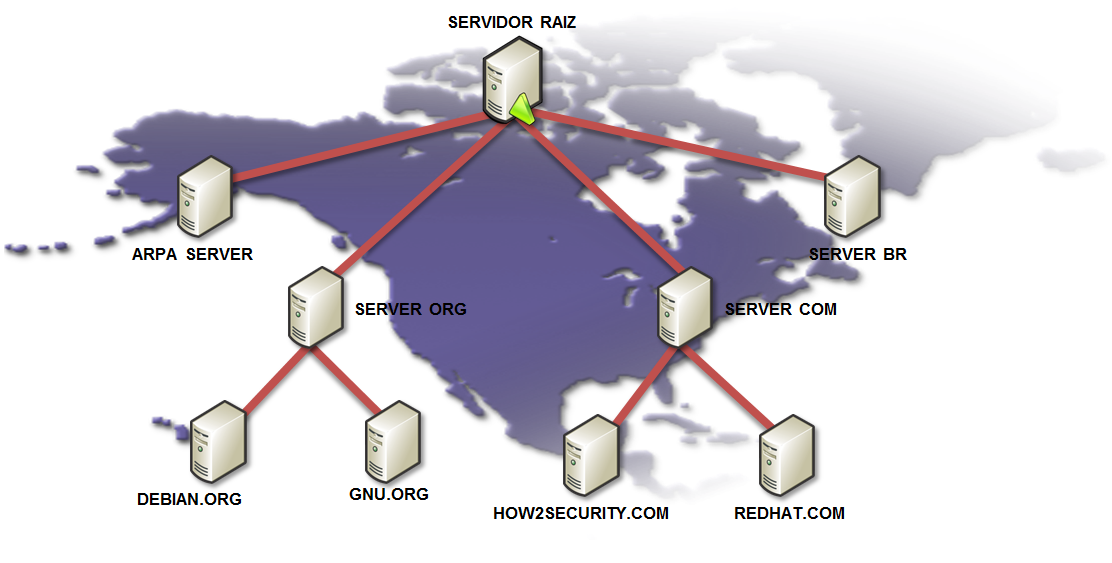


Figura 04 – Hierarquia de Servidores e Nomes

**1.3.2 – Zonas**

Uma zona é uma porção administrativa de um domínio **DNS**, e aceita as responsabilidades do domínio e não cria subdomínios, o domínio e o subdomínio e a zona são as mesmas coisas.

Porém se subdividimos um domínio em porções menores (subdomínios) delegamos a autoridade do domínio para outros servidores. Daí o domínio e a zona se tornam coisas diferentes.

Desta forma o detalhamento do domínio fica armazenado em servidores de níveis mais baixos.

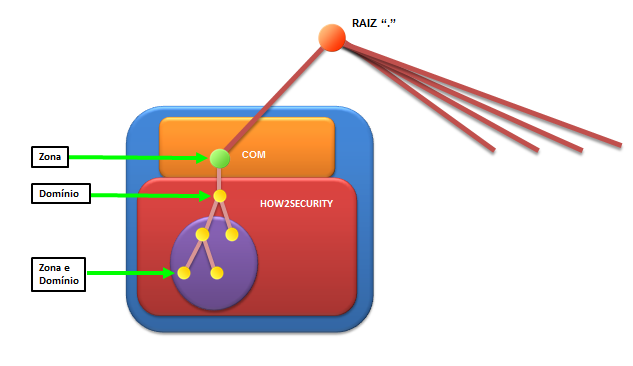


Figura 05 – Zonas e Domínio

**1.3.3 – Servidor Raiz**

Um servidor raiz é um servidor onde consiste em toda árvore. O servidor raiz não armazena nenhuma informação sobre os subdomínios, apenas delega autoridade a outros servidores, fazendo referência a eles. Eles estão espalhados por vários locais ao redor do mundo.

**1.3.4 – Servidores Primários e Secundários**

O **DNS** define dois tipos de servidores, **o Servidor DNS Primário** e o **Servidor DNS Secundário**.

Ambos servidores tem a autoridade sobre a zona ao qual eles servem. Assim criando uma redundância do banco de dados do **DNS**, em caso de falha do **Servidor DNS Primário** o **Servidor DNS Secundário** tem plenas condições de atender as requisições dos clientes.

A diferencia entre os **DNS Primários** e o **Secundários** são:

* **Servidor DNS Primário** 🡪 Armazena no disco local as informações sobre a zona que tem autoridade. Ele é o responsável por criar, manter e atualizar os arquivos de zona. Todas as alterações devem ser feitas nele, e ele é responsável pela replicação entre os **Servidores DNS Secundários**.
* **Servidor DNS Secundário** 🡪 Ele recebe as informações sobre a zona de outro servidor (**Primário** ou **Secundário**) e armazena em seu disco local. Este servidor é somente leitura, não podendo alterar seus arquivos de zona local.

**2 – Mensagens DNS**

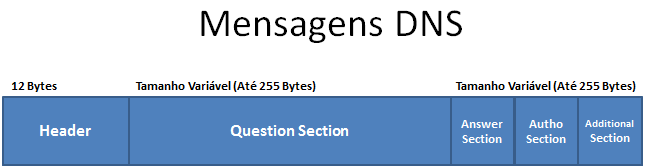


Figura 01 – Mensagem DNS

**2.1 – Header das Mensagens DNS (Cabeçalho)**

O **DNS** tem dois tipos de mensagens: de consulta e de resposta, ambas têm o mesmo formato.

No cabeçalho das mensagens DNS de consulta temos o uso de dois campos o **Header** e o **Question**, já na resposta temos o uso de cinco campos o **Header**, **Question**, **Answer**, **Autority** e **Additional**.

Aqui iremos ver os campos que compõe o **Header**, seu tamanho é de **12 bytes**, e se for uma mensagem de consulta ela tem alguns campos zerados, seu formato é demostrado na **Figura 01.**

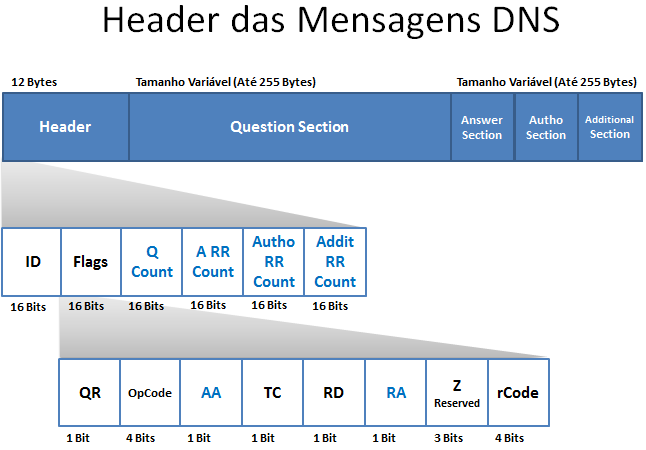


Figura 02 – Header das Mensagens DNS

Os campos são preenchidos da seguinte forma:

* **Identification (Identificação)** 🡪 Esse é um campo de **16 bits** usados pelo cliente para identificar qual resposta corresponde à consulta, o servidor duplica esse número na resposta correspondente a consulta.
* **Flags** 🡪 Esse é um campo de **16 bits** que consiste em outros subcampos, são eles:
  + **QR (Consulta/Resposta)** 🡪 Esse é um subcampo de **1 bit** que define o tipo de mensagem. Se for **0 (zero)**, a mensagem é uma consulta. Se for **1 (um)**, a mensagem é uma resposta.
  + **OpCode** 🡪 Esse é um subcampo de **4 bits** que define o tipo de consulta ou resposta.

|  |  |
| --- | --- |
| Valor | Significado |
| 0 | QUERY 🡪 Consulta Padrão |
| 1 | IQUERY 🡪 Consulta Inversa |
| 2 | STATUS 🡪 Pedido de Status do Servidor |
| 3 – 15 | Reservado para uso futuro |

Tabela 01 - OpCode

* + **AA (Resposta Autorizada)** 🡪 Esse é um subcampo de **1 bit**. Quando seu valor for **1 (um)** significa que o servidor de nomes é um servidor autorizado. Ele é utilizado apenas em **mensagens de respostas**.
  + **TC (Truncado)** 🡪 Esse é um subcampo de **1 bit**. Quando seu valor for **1 (um)** significa que a resposta tinha mais que **512 bytes** e foi truncada devido o canal de transmissão utilizado (**UDP**) tem tamanho inferior a **512 bytes**.
  + **RD (Recursividade Desejada)** 🡪 Esse é um subcampo de **1 bit**. Quando seu valor for **1 (um)** significa que o cliente deseja uma resposta recursiva. Ele é configurado na mensagem de consulta e repetido na mensagem de resposta.
  + **RA (Recursividade Disponível)** 🡪 Esse é um subcampo de **1 bit**. Quando é configurado na resposta significa que o servidor responderá a recursivamente. Este subcampo está presente apenas nas mensagens de respostas.
  + **Z (Reservado)** 🡪 Esse é um subcampo de **3 bits** configurado como **000**.
  + **RCode** 🡪 Esse é um subcampo de **4 bits** que mostra o status de erro da resposta. Somente um servidor autorizado pode entregar essa resposta. Seus valores são:

|  |  |
| --- | --- |
| Valor | Significado |
| 0 | Nenhum Erro |
| 1 | Erro de Formato |
| 2 | Problema no Servidor de Nomes |
| 3 | Problema de Referência de Domínio |
| 4 | Tipo de Consulta não Suportado |
| 5 | Proibido Administrativamente (Politicas) |
| 6 – 15 | Reservados |

Tabela 02 - RCode

* **QD Count (Contador de Registros de Perguntas)** 🡪 Esse é um campo de **16 bits** que contém um contador de consultas na seção de perguntas da mensagem.
* **AN Count (Contador de Registro de Resposta)** 🡪 Esse é um campo de **16 bits** que contém um contador de registros de resposta na seção de respostas da mensagem de resposta. Seu valor é zerado em uma mensagem de consulta.
* **NS Count (Contador de Registros Autorizados)** 🡪 Esse é um campo de **16 bits** que contém um contador de registros autorizados na seção autorizada das mensagens de respostas. Seu valor é zerado em uma mensagem de consulta.
* **AR Count (Contador de Registros Adicionais)** 🡪 Esse é um campo de **16 bits** que contém um contador de registros adicionais na seção adicionais de uma mensagem de resposta. Seu valor é zerado em uma mensagem de consulta.

**2.2 – Question Section das Mensagens DNS**

O campo **Question Section (Seção de Pergunta)** é utilizado pelo cliente para transmitir informações referentes à consulta para o servidor. Seu formato é demostrado na **Figura 03**.

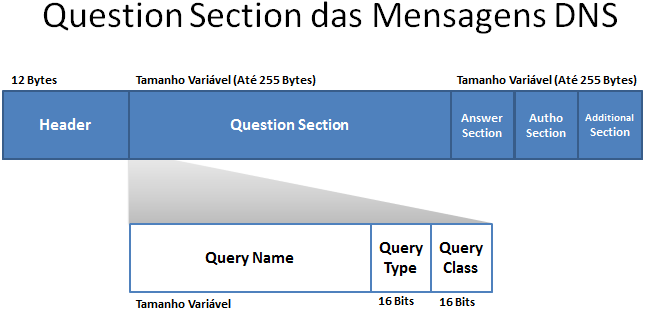


Figura 03 – Formato do Campo Question Section

Ele contém três subcampos, são eles:

* **Query Name (Nome da Consulta)** 🡪 Esse é um campo de tamanho variável que contém uma série de rótulos (**label**) que consiste do nome de domínio ou um endereço IP. O nome do domínio é codificado com uma série de pares de tamanho e valor que indica o tamanho do rótulo seguido do rótulo e finalizando com uma **string** nula indicando o root. Por exemplo, no domínio [**www.how2security.com.br**](http://www.how2security.com.br)**,** este domínio seria expresso da seguinte forma: ***0x03www0x0Chow2security0x03com0x02br0x00***, onde os dígitos hexadecimais representam o tamanho de cada rótulo e os caracteres **ASCII** indicam os rótulos individuais e o final **0x00** indica o final do nome (**root**).
* **Query Type (Tipo de Pergunta)** 🡪 Esse é um subcampo de **16 bits** que define o tipo de consulta. Na **Tabela 03** temos os principais tipos de registros usados em uma consulta.

|  |  |  |
| --- | --- | --- |
| Tipo | Mnemônico | Descrição |
| 01 - (0x01) | A | Endereço. Um Endereço IPv4 de 32 bits. É utilizado para converter um nome de domínio em um endereço IP. |
| 02 - (0x02) | NS | Servidor de Nomes. Identifica os servidores autorizados para uma zona. |
| 03 - (0x03) | MD | Um e-mail de destino (Mail Destination). |
| 04 - (0x04) | MF | Um encaminhador de e-mail (Mail Fowarder). |
| 05 - (0x05) | CNAME | Nome Canônico. Identifica um pseudônimo (alias) para um nome de um host. |
| 06 - (0x06) | SOA | Inicio de Autoridade. Marca o início de uma zona. |
| 11 -(0x0B) | WKS | Serviços Conhecidos. Define os serviços de rede que o host oferece. |
| 12 - (0x0C) | PTR | Ponteiro. Usado para converter um endereço IP em um nome de domínio. |
| 13 - (0x0D) | HINFO | Informações do Host. Fornece a descrição de hardware e do sistema operacional usado por um host. |
| 14 – (0x0E) | MINFO | Informações sobre mailbox ou mail list. |
| 15 - (0x0F) | MX | Troca de Correspondência. Redireciona os e-mails para um servidor de correio. |
| 16 – (0x10) | TXT | Série de caracteres. |
| 28 - (0x1C) | AAAA | Endereço. Um endereço IPv6. |
| 33 - (0x21) | SRV | Registros de Serviços. |
| 251 - (0xFB) | IXFR | Um pedido de transferência de zona incremental. |
| 252 - (0xFC) | AXFR | Um pedido para a transferência da zona inteira. |
| 255 - (0xFF) | ANY | Um pedido de todos os registros. |

Tabela 03 – Tipos de Pergunta

* **Query Class (Classe da Pergunta)** 🡪 Esse é um subcampo de **16 bits** que define o protocolo específico usando no DNS.

|  |  |  |
| --- | --- | --- |
| Classe | Mnemônicos | Descrição |
| 1 | IN | Internet |
| 2 | CSNET | Rede CSNET (obsoleta) |
| 3 | CS | A rede COAS |
| 4 | HS | Servidor Hesiod Desenvolvido pelo MIT. |

Tabela 04 – Classes de Pergunta

**2.3 – Resources Records das Mensagens DNS**

As seções de resposta, autoridade e adicionais (**Answer**, **Authority** e **Additional**) compartilham o mesmo formato. Cada nome de domínio é associado a um registro chamado **Resouce Records (RRs)**.

O número de **RRs** é especificado no campo correspondente dos contadores dentro do cabeçalho DNS. E todos os **RR** tem o seguinte formato:

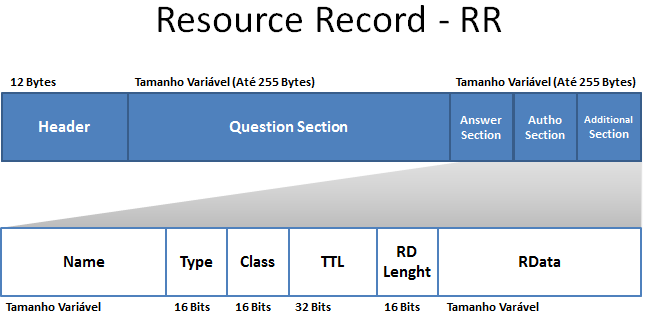


Figura 04 – Formato do RR

Agora vamos à descrição de cada campo:

* **Name (Nome do Domínio)** 🡪 Esse é um campo de comprimento variável que contém o nome do domínio. É uma cópia do nome do domínio presente no **Query Name** do **Question Section**. O DNS faz uso da compactação em todo lugar em que um nome é repedido, esse campo é um ponteiro que desloca para o início do campo **Query Name**.
* **Type (Tipo de Domínio)** 🡪 Esse campo é igual ao campo **Query Type** do **Question Section**.
* **Class (Classe do Domínio)** 🡪 Esse campo é igual ao campo **Query Class** do **Question Section**.
* **TTL – Time to Life (Tempo de Vida)** 🡪 Esse é um campo de **32 bits** que define em segundos o tempo em que a resposta é válida. Esse valor também é utilizado para manter o registro em cache. Um valor zerado significa que este registre só é valido para essa consulta.
* **RD Lenght (Comprimento dos Dados do Recurso)** 🡪 Esse é um campo de **16 bits** que define o comprimento dos dados do recurso.
* **RData (Dados do Recurso)** 🡪 Esse é um campo de tamanho variável que contém a resposta para a consulta (**Answer Section**), o nome de domínio do servidor autorizado (**Authority Section**) ou informações adicionais (**Additional Section**). Ele pode conter os seguintes dados:
  + **IP Address (Endereço IP)** 🡪 Ele é escrito em octetos. Se for **IPv4** serão **4** octetos ou se for **IPv6** **16** octetos.
  + **Domain Name (Nome de Domínio)** 🡪 Os nomes de domínio são expressos como uma sequência de rótulos. Cada rótulo é precedido de um campo de comprimento de **1 byte** que define o número de caracteres presente no rótulo. E para identificar o final dos caracteres ele é sinalizado por uma **string** **nula** **(0x00)**. Para distinguir um campo de comprimento de um ponteiro de deslocamento, os **2 bits** mais significativos do byte estão zerados (**00**). Como o comprimento máximo de um rótulo é **63 bytes** ele usará apenas os **6 bits** menos significativos do byte **(Binário = 11111|Byte = 00111111|Hexa = 0x3F|Dec = 63)**. Enquanto o ponteiro de deslocamento ficaria com um valor de **192** **(Binário e Byte= 11000000|Hexa = 0xC0|Dec = 192)**.
  + **Dereference Pointer (Ponteiro de Deslocamento)** 🡪 Os nomes de domínio repetidos podem utilizar um ponteiro. Ficando com algo como **0xC00C** que são divididos em dois valores **0xC0** significando que o próximo dado se refere a um ponteiro de deslocamento e o ponteiro **0x0C** apontando para o final do cabeçalho que tem **12 bytes** de comprimento.
  + **Strings (Série de Caracteres)** 🡪 Uma série de caracteres é representada por um campo de comprimento de **1 byte**, seguido do número de caracteres definido no campo comprimento. Essa série de caracteres pode conter até **255 caracteres** incluindo o comprimento das séries de caracteres.

|  |  |
| --- | --- |
| Parâmetros | Limite |
| Label (Rótulos) | Até 63 octetos. |
| Names (Nomes) | Até 255 octetos. |
| TTL (Tempo de Vida) | Valor inteiro positivo de até 32 bits (4 octetos). |
| UDP (Mensagens UDP) | Até 512 octetos. |

Tabela 05 – Limite de Tamanho dos Parâmetros em Mensagens DNS

**2.4 – Compactação nas Mensagens DNS**

Para reduzir o tamanho das mensagens DNS, o DNS utiliza um esquema de compressão, assim eliminando as repetições de nomes de domínios dentro de suas mensagens. Para isso, ele utiliza **2 bytes (16 bits)**, sendo os **2 bits** mais significativos utilizados para sinalizar que os próximos **14 bits** menos significativos é um **OFFSET** de deslocamento (um ponteiro) apontando para o início do nome de domínio repetido.

O formato de um ponteiro é:

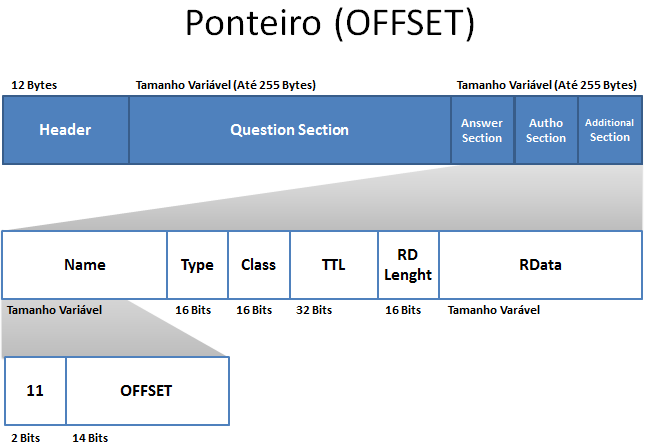


Figura 05 – Formato do Ponteiro

Para distinguir um campo de comprimento de um ponteiro de deslocamento, os **2 bits** mais significativos do byte estão zerados (**00**). Como o comprimento máximo de um rótulo é 63 bytes ele usará apenas os **6 bits** menos significativos do byte **(Binário = 11111|Byte = 00111111|Hexa = 0x3F|Dec = 63)**. Enquanto o ponteiro de deslocamento ficaria com um valor de **192** **(Binário e Byte= 11000000|Hexa = 0xC0|Dec = 192)**. E o valor Binário dos **2 Bytes** ficaria **1100000000001100** ou em Hexa **0xC00C**, indicando que a próxima informação é um ponteiro e que seu deslocamento será **12 Bytes** a partir do início do cabeçalho.

**2.5 – Analisar as Mensagens DNS**

Aqui irei reproduzir uma consulta recursiva e outra consulta reversa para entendermos as mensagens DNS. Nosso **Cliente DNS** irá pesquisar o nome de domínio [**www.how2security.com.br**](http://www.how2security.com.br) para nos retornar o **endereço IP**.

Vamos olhar o cabeçalho capturado com o **Wireshark** e depois uma ilustração do cabeçalho:

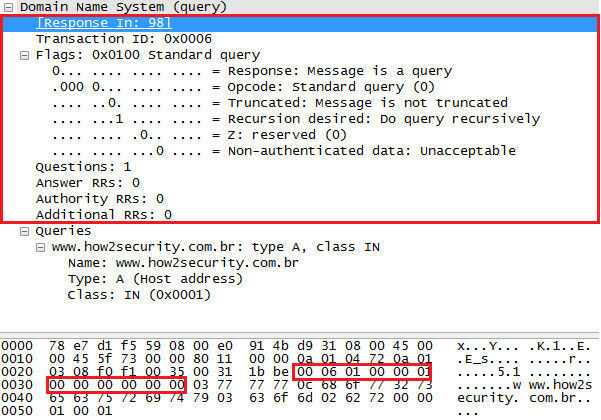


Figura 06 – Cabeçalho da Mensagem DNS de Query Capturada com o Wireshark

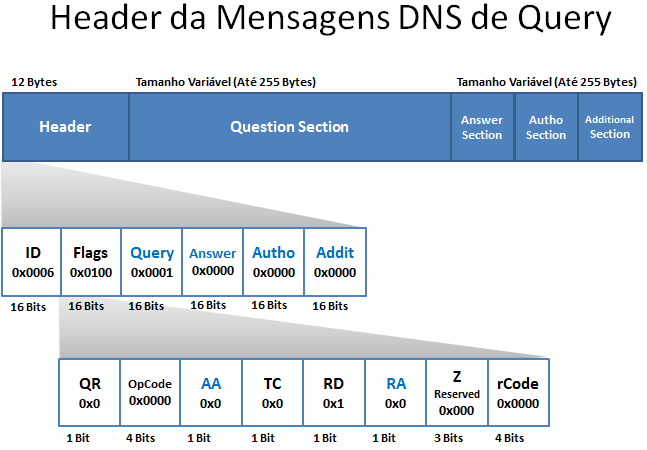


Figura 07 – Ilustração do Cabeçalho da Mensagem DNS

A **Figura 06** mostra a consulta feita do **Cliente DNS** para um servidor local. Em seu cabeçalho temos o **ID** da consulta **0x06**, ele é um número sequencial que relaciona uma pergunta a uma resposta. Os Bytes seguintes contêm os valores das **Flags** que em **Hexa** é **0x0100,** e em **Binário** **0000000100000000**, e que tem seus campos correspondentes na figura de ilustração do cabeçalho (**Figura 07**). Observe que o subcampo **QR** define a mensagem como uma consulta (**0x0**) e o bit de recursividade ativo em **RD** (**0x1**).

Agora vamos observar a **Query Section** nas figuras abaixo:

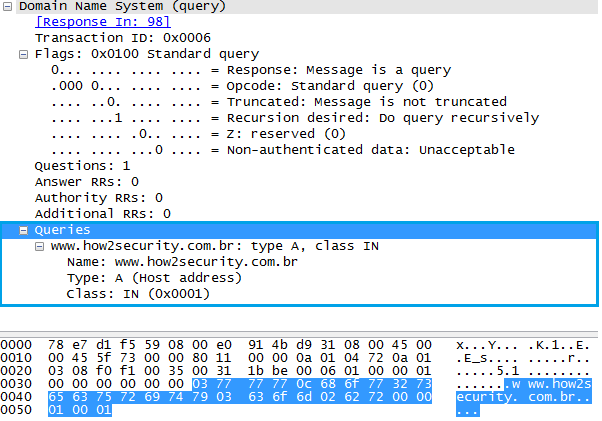


Figura 08 – Seção de Pergunta da Mensagem DNS de Query Capturada com o Wireshark

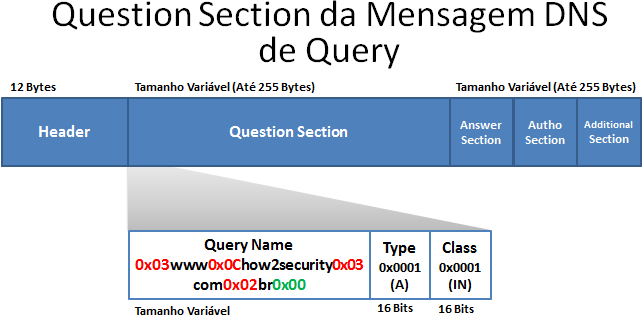


Figura 09 - Ilustração da Seção de Pergunta da Mensagem DNS

O nome do domínio é **0x03www0x0Chow2security0x03com0x02br0x00** onde temos, os comprimentos dos rótulos **(Labels)** e o próprio rótulo finalizando com um byte nulo **(Null Byte = 0x00)**. Em seguida temos mais dois bytes indicando o tipo de consulta **(A)** e a classe com a Internet **(IN)**.

Agora vamos analisar a resposta do **Servidor DNS**.

**Observação:** Lembre-se que o cabeçalho se repete então não irei repeti-lo, apenas apresentar o que foi alterado na resposta que basicamente são as **Flags** e **Answer**.

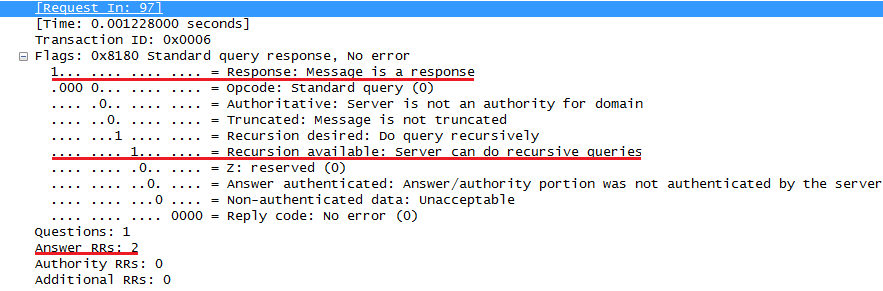


Figura 10 – Diferença do Cabeçalho de Resposta

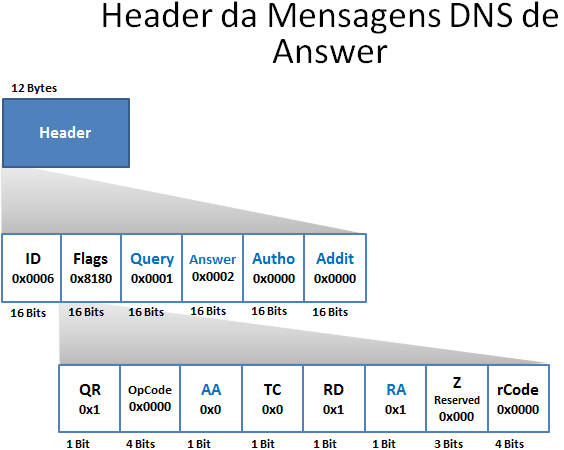


Figura 11 – Ilustração do Cabeçalho de Resposta da Mensagem DNS

No cabeçalho temos o valor **0x8180** para as **Flags** sinalizando o **QR** como resposta (**0x1**), o bit de **RD** (recursividade disponível) ativo (**0x1**). Além de informar que existem duas respostas (**Answer** com o valor **0x0002**), pois solicitamos uma consulta do tipo **A** e o nome de domínio informado diz respeito a um Alias (**CNAME**).

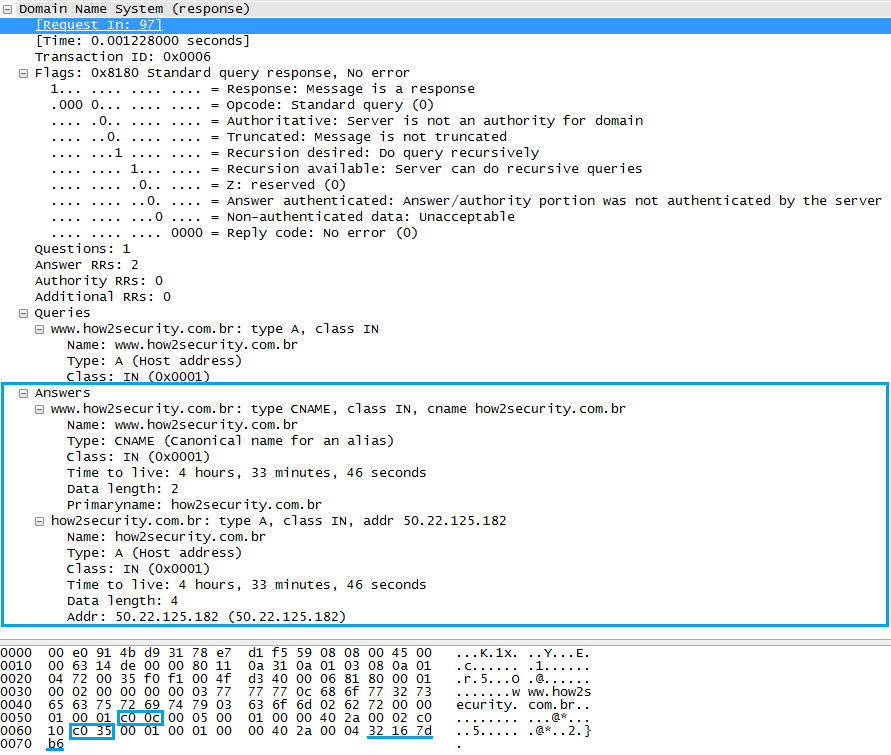


Figura 12 - Seção de Resposta da Mensagem DNS de Respostar Capturada com o Wireshark

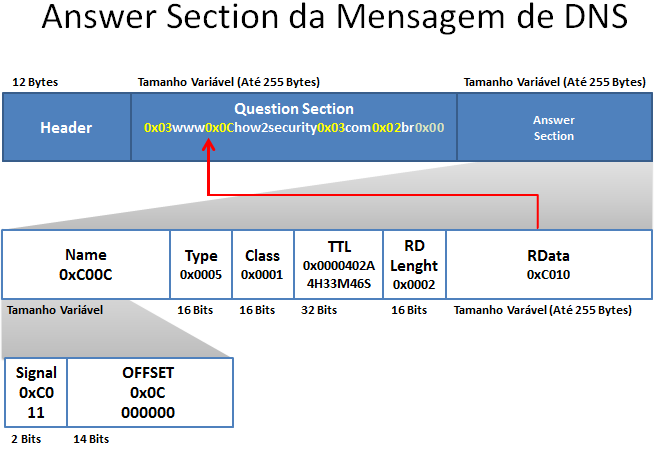


Figura 14 - Ilustração da Primeira Parte Resposta da Mensagem DNS

Já na **Seção de Resposta**, temos duas respostas a nossa consulta, a primeira indica que temos um ponteiro de deslocamento e em seguida o endereço de deslocamento. Os dois bits mais significativos em **Name**, indica o ponteiro (**11** ou **0xC0 – Binário/Hexa**) e em seguida o valor de deslocamento que são **12 Octetos** a partir do início do cabeçalho (lembrando que inicia no endereço **0x00** e termina no endereço **0x0B**, ele aponta exatamente para o início da **Question Section** onde temos o comprimento do primeiro rótulo).

Em seguida temos o campo **Type** com o valor **0x005** que se refere a um registro do tipo **CNAME**, que pertence à classe **Internet** informado no campo **Class** (**0x01**). O campo com o valor **0x0000402A** é o **TTL** (4 horas 33 minutos e 46 segundos), que informa por quanto tempo este registro ficará em cache. O campo **RD Lenght (Comprimento do Campo Response Data)** informa o comprimento da resposta (**2 Bytes** ou **0x02**), Em seguida temos novamente um ponteiro de deslocamento (**0x10**) e que desloca **16 Bytes** a partir do cabeçalho, já que o nome do tipo **A** do host é **how2security.com.br**, iniciando exatamente onde temos o comprimento do segundo rótulo.

A segunda parte é a resposta da resolução do endereço IP do host (que foi nossa solicitação inicial).

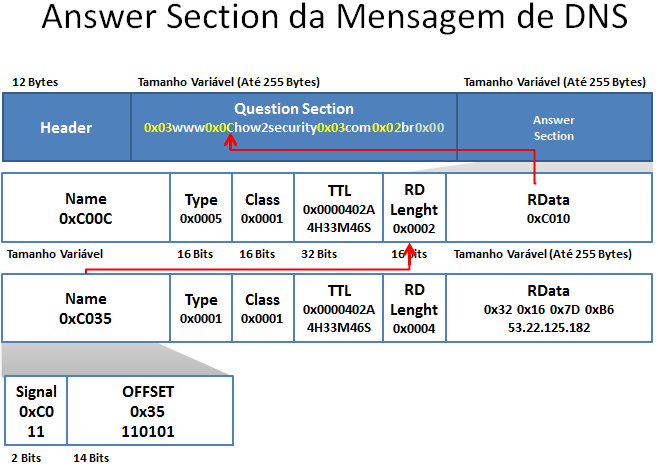


Figura 14 - Ilustração da Segunda Parte Resposta da Mensagem DNS

Aqui temos o **Name**, que já podemos observar que indica um ponteiro de deslocamento e em seguida o endereço de deslocamento. Os dois bits mais significativos como já sabemos, indica o ponteiro (**11** ou **0xC0**) e em seguida o valor de deslocamento que são **53 Octetos** a partir do início do cabeçalho. Aqui vale lembrar que as mensagens DNS comprime todos os campos que se repete, então nosso deslocamento vai exatamente para o comprimento da resposta que por sua vez indica o tamanho do campo **RData** que também é um deslocamento para o segundo comprimento do segundo rótulo que é o nome do host.

Em seguida temos o campo **Type** com o valor **0x001** que se refere a um registro do tipo **A**, que pertence à classe **Internet**, informado no campo **Class** (**0x01**). O campo com o valor **0x0000402A** é o **TTL** (4 horas 33 minutos e 46 segundos), que informa por quanto tempo este registro ficará em cache. O campo **RD Lenght** (Comprimento do campo **Response Data**) informa o comprimento da resposta (**4 Bytes** ou **0x04**), Em seguida temos a resolução do nome para o endereço que é **53.22.125.182** **(0x32 0x16 0x7D 0xB6)**.

Irei apenas ilustrar a consulta do reverso, já que ele segue o mesmo princípio da resolução recursiva. A diferença fica por conta do tipo, que em vez de resolver o nome de domínio, queremos resolver o endereço IP para nome de domínio.

Logo abaixo temos as figuras de capturadas do **Header (Cabeçalho)** e da **Question Section (Seção de Pergunta)**.

Vale lembrar que o endereço IP que estamos consultando é o **50.22.125.182** e no campo **Name** ele vai invertido, sendo cada **Octeto** interpretado como uma **String**, ou seja, o valor **50** são **dois Bytes**, além dos acréscimos das hierarquias de primeiro e segundo níveis (**arpa** e **in-addr** respectivamente).

Vejamos o Cabeçalho:

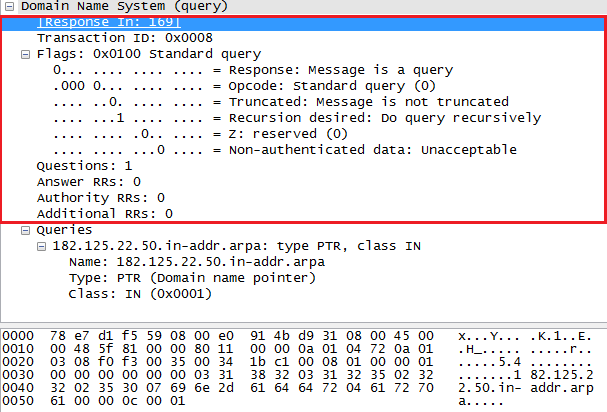


Figura 15 – Seção de Pergunta da Mensagem DNS de Query Reverso Capturada com o Wireshark

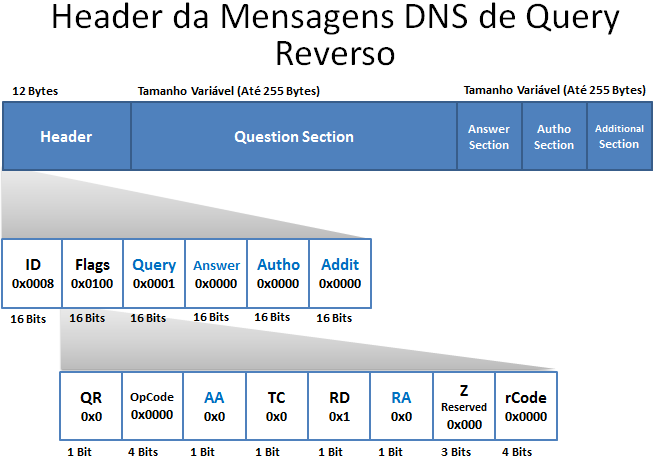


Figura 16 – Ilustração da Seção de Pergunta Reverso da Mensagem DNS

Agora a Seção de Pergunta:

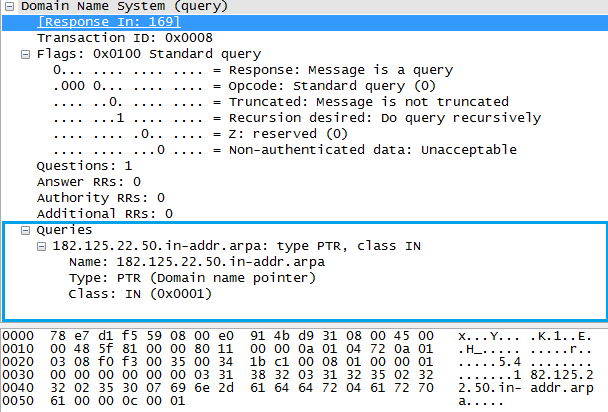


Figura 17 – Seção de Pergunta da Mensagem DNS de Query Capturada com o Wireshark

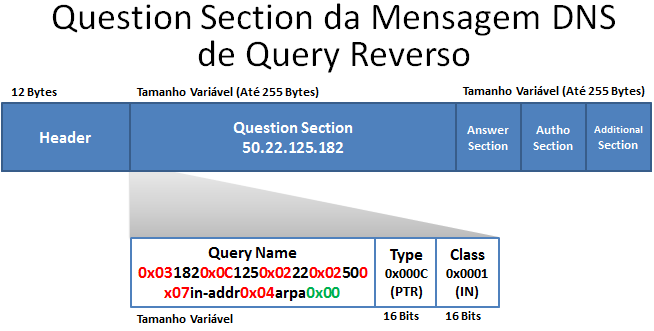


Figura 18 – Ilustração da Seção de Pergunta da Mensagem DNS

Agora iremos ver a Resposta:

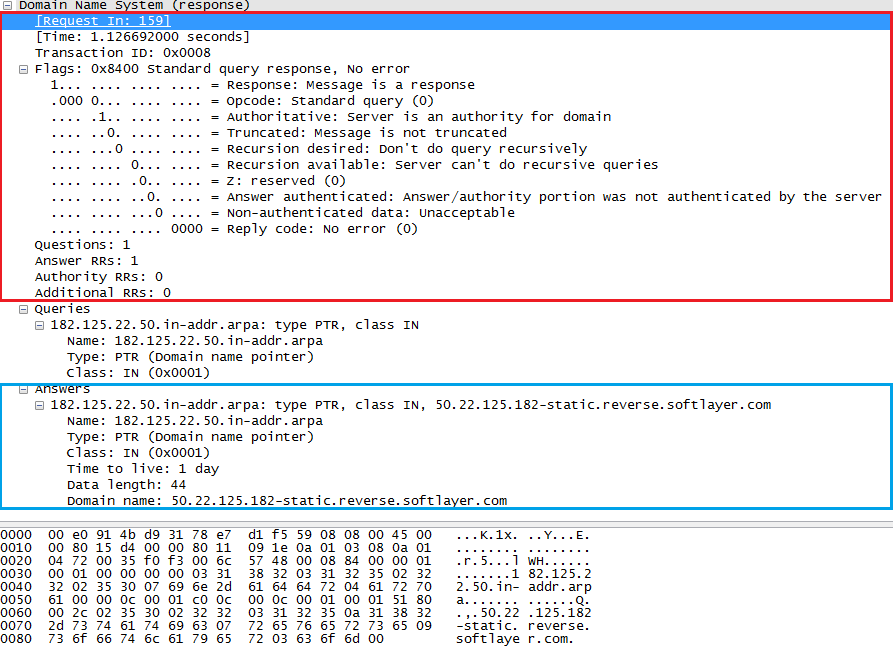


Figura 19 – Seção de Resposta da Mensagem DNS de Resposta Capturada com o Wireshark

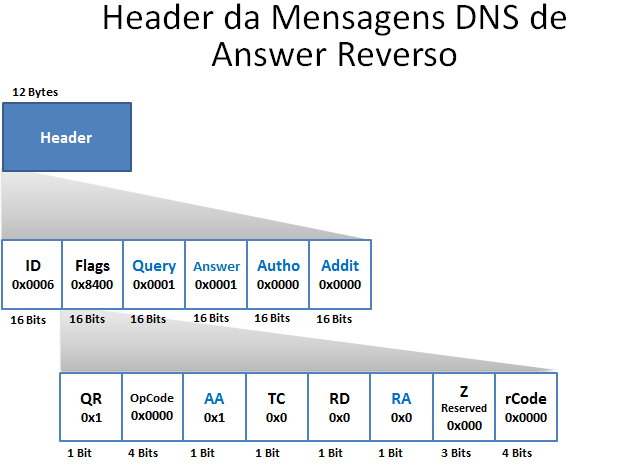


Figura 20 – Ilustração do Cabeçalho de Resposta da Mensagem DNS

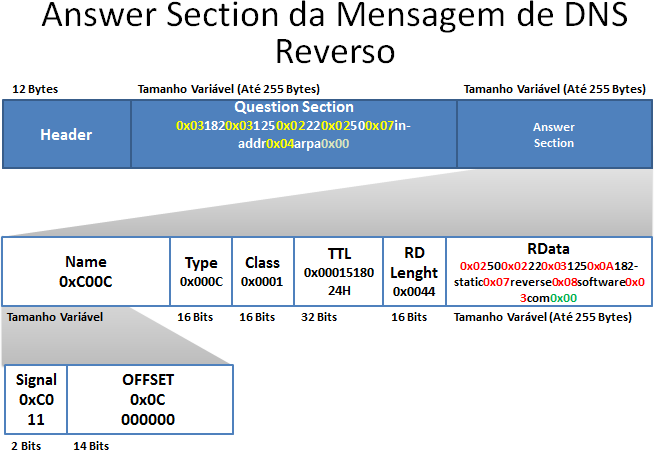


Figura 21 - Ilustração da Resposta da Mensagem DNS

**3 – DNS na Internet**

O **DNS** na Internet é dividido em três seções diferentes, são elas: domínios genéricos, domínio de país e domínio inverso.

**3.1 – Domínios Genéricos**

Os domínios genéricos descrevem os tipos de organizações pelo registro, que servem como um índice para um banco de dados de espaço de nomes.

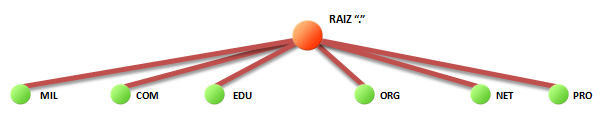


Figura 01 – Domínios Genéricos

Veja alguns exemplos na tabela abaixo:

|  |  |
| --- | --- |
| Rótulo | Descrição |
| .com | Atividades comerciais |
| .eco | Atividades com foco eco-ambiental |
| .emp | Pequenas e micro-empresas |
| .net | Atividades comerciais |
| .blog | Web logs |
| .flog | Foto logs |
| .nom | Pessoas físicas |
| .vlog | Vídeo logs |
| .wiki | Páginas do tipo wiki |
| .edu | Instituições de ensino superior |
| .adm | Administradores |
| .adv | Advogados |
| .arq | Arquitetos |
| .ato | Atores |
| .bio | Biólogos |
| .bmd | Biomédicos |
| .cim | Corretores |
| .cng | Cenógrafos |
| .cnt | Contadores |
| .ecn | Economistas |
| .eng | Engenheiros |
| .eti | Especialistas em Tecnologia da Informação |
| .fnd | Fonoaudiólogos |
| .fot | Fotógrafos |
| .fst | Fisioterapeutas |
| .gcf | Geógrafos |
| .jor | Jornalistas |
| .lel | Leiloeiros |
| .mat | Matemáticos e Estatísticos |
| .med | Médicos |
| .mus | Músicos |
| .not | Notários |
| .ntr | Nutricionistas |
| .odo | Dentistas |
| .ppg | Publicitários e profissionais da área de propaganda e marketing |
| .pro | Professores |
| .psc | Psicólogos |
| .qsl | Rádio amadores |
| .slg | Sociólogos |
| .taxi | Taxistas |
| .teo | Teólogos |
| .trd | Tradutores |
| .vet | Veterinários |
| .zlg | Zoólogos |
| .agr | Empresas agrícolas, fazendas |
| .art | Artes: música, pintura, folclore |
| .esp | Esporte em geral |
| .etc | Empresas que não se enquadram nas outras categorias |
| .far | Farmácias e drogarias |
| .imb | Imobiliária |
| .ind | Indústrias |
| .inf | Meios de informações (rádios, jornais, bibliotecas, etc) |
| .radio | Empresas que queiram enviar áudio pela rede |
| .rec | Atividades de entretenimento, diversão, jogos, etc. |
| .srv | Empresas prestadoras de serviços |
| .tmp | Eventos temporários, como feiras e exposições |
| .tur | Empresas da área de turismo |
| ..tv | Empresas de radiodifusão de sons e imagens |
| .am | Empresas de radiodifusão sonora |
| .coop | Cooperativas |
| .fm | Empresas de radiodifusão sonora |
| .g12 | Instituições de ensino de primeiro e segundo grau |
| .gov | Instituições do governo federal |
| .mil | Forças Armadas/Militares |
| .org | Instituições não governamentais sem fins lucrativos |
| .psi | Provedores de serviços de Internet |
| .b | Bancos |
| .jus | Instituições do Poder Judiciário |
| .leg | Instituições do Poder Legislativo |
| .mp | Instituições do Ministério Público |

Tabela 01 – Rótulos de domínios genéricos

**3.2 – Domínios de País**

A seção de domínios de país usa abreviatura de países com dois caracteres, além de utilizaram subdomínio como abreviação para estados. Por exemplo, o Brasil utiliza **.br** e **sp.br** para indicar São Paulo – Brasil. Observam a tabela abaixo com as abreviações dos países.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | País | Country | Bandeira |
| .ac | Ilhas Ascensão |  | Flag of Ascension Island.svg |
| .ad | Andorra | Andorra | http://www.gregoriano.org.br/portinha/ad.gif |
| .ae | Emirados Árabes Unidos | United Arab Emirates | http://www.gregoriano.org.br/portinha/ae.gif |
| .af | Afeganistão | Afghanistan | http://www.gregoriano.org.br/portinha/af.gif |
| .ag | Antígua e Barbuda | Antigua and Barbuda | http://www.gregoriano.org.br/portinha/ag.gif |
| .ai | Anguilla | Anguilla | http://www.gregoriano.org.br/portinha/ai.gif |
| .al | Albânia | Albania | http://www.gregoriano.org.br/portinha/al.gif |
| .am | Arménia | Armenia | http://www.gregoriano.org.br/portinha/am.gif |
| .an | Antilhas Holandesas | Netherlands Antilles | http://www.gregoriano.org.br/portinha/an.gif |
| .ao | Angola | Angola | http://www.gregoriano.org.br/portinha/ao03.gif |
| .aq | Antártida | Antarctica | http://www.gregoriano.org.br/portinha/aq-g.gif |
| .ar | Argentina | Argentina | http://www.gregoriano.org.br/portinha/ar.gif |
| .as | Samoa Americana | American Samoa | http://www.gregoriano.org.br/portinha/as.gif |
| .at | Áustria | Austria | http://www.gregoriano.org.br/portinha/at.gif |
| .au | Austrália | Australia | http://www.gregoriano.org.br/portinha/au.gif |
| .aw | Aruba | Aruba | http://www.gregoriano.org.br/portinha/aw.gif |
| .az | Azerbaijão | Azerbaijan | http://www.gregoriano.org.br/portinha/az.gif |
| .ba | Bósnia e Herzegovina | Bosnia and Barbuda | http://www.gregoriano.org.br/portinha/ba.gif |
| .bb | Barbados | Barbados | http://www.gregoriano.org.br/portinha/bb.gif |
| .bd | Bangladesh | Bangladesh | http://www.gregoriano.org.br/portinha/bd.gif |
| .be | Bélgica | Belgium | http://www.gregoriano.org.br/portinha/be.gif |
| .bf | Burkina Faso | Burkina Fase | http://www.gregoriano.org.br/portinha/bf.gif |
| .bg | Bulgária | Bulgaria | http://www.gregoriano.org.br/portinha/bg.gif |
| .bh | Bahrein | Bahrain | http://www.gregoriano.org.br/portinha/bh.gif |
| .bi | Burundi | Burundi | http://www.gregoriano.org.br/portinha/bi.gif |
| .bj | Benin | Benin | http://www.gregoriano.org.br/portinha/bj.gif |
| .bm | Bermudas | Bermuda | http://www.gregoriano.org.br/portinha/bm.gif |
| .bn | Brunei Darussalam | Brunei Darussalam | http://www.gregoriano.org.br/portinha/bn.gif |
| .bo | Bolívia | Boliva | http://www.gregoriano.org.br/portinha/bo.gif |
| .br | Brasil | Brazil | http://www.gregoriano.org.br/portinha/br.gif |
| .bs | Bahamas | Bahamas | http://www.gregoriano.org.br/portinha/bs.gif |
| .bt | Butão | Bhutan | http://www.gregoriano.org.br/portinha/bt.gif |
| .bv | Ilhas Bouvet | Bouvet Island | http://www.gregoriano.org.br/portinha/bv.gif |
| .bw | Botswana | Botswana | http://www.gregoriano.org.br/portinha/bw.gif |
| .by | Bielorrúsia | Belarus | http://www.gregoriano.org.br/portinha/by.gif |
| .bz | Belize | Belize | http://www.gregoriano.org.br/portinha/bz.gif |
| .ca | Canadá | Canada | http://www.gregoriano.org.br/portinha/ca.gif |
| .cc | Ilhas Cocos | Cocos (Keeling) Islands | http://www.gregoriano.org.br/portinha/cc.gif |
| .cd | República Democrática do Congo |  | Bandeira da República Democrática do Congo |
| .cf | República Centro Africana |  | http://www.gregoriano.org.br/portinha/cf.gif |
| .cg | Congo |  | http://www.gregoriano.org.br/portinha/cg.gif |
| .ch | Suíça | Switzerland | http://www.gregoriano.org.br/portinha/ch.gif |
| .ci | Costa do Marfim |  | http://www.gregoriano.org.br/portinha/ci.gif |
| .ck | Ilhas Cook | Cook Islands | http://www.gregoriano.org.br/portinha/ck.gif |
| .cl | Chile | Chile | http://www.gregoriano.org.br/portinha/cl.gif |
| .cm | Camarões | Cameroon | http://www.gregoriano.org.br/portinha/cm.gif |
| .cn | República Popular da China | China | http://www.gregoriano.org.br/portinha/cn.gif |
| .co | Colômbia | Colombia | http://www.gregoriano.org.br/portinha/co.gif |
| .cr | Costa Rica |  | http://www.gregoriano.org.br/portinha/cr.gif |
| .cu | Cuba | Cuba | http://www.gregoriano.org.br/portinha/cu.gif |
| .cv | Cabo Verde | Cape Verde | http://www.gregoriano.org.br/portinha/cv.gif |
| .cx | Ilhas Natal | Christmas Island | http://www.gregoriano.org.br/portinha/cx.gif |
| .cy | Chipre | Cyprus | http://www.gregoriano.org.br/portinha/cy.gif |
| .cz | República Theca | Czech Republic | http://www.gregoriano.org.br/portinha/cz.gif |
| .de | Alemanha | Deutschland (Germany) | http://www.gregoriano.org.br/portinha/de.gif |
| .dj | Djibouti | Djibouti | http://www.gregoriano.org.br/portinha/dj.gif |
| .dk | Dinamarca | Denmark | http://www.gregoriano.org.br/portinha/dk.gif |
| .dm | Dominica | Dominica | http://www.gregoriano.org.br/portinha/dm.gif |
| .do | República Dominicana | Dominican Republic | http://www.gregoriano.org.br/portinha/do.gif |
| .dz | Argélia | Algeria | http://www.gregoriano.org.br/portinha/dz.gif |
| .ec | Equador | Ecuador | http://www.gregoriano.org.br/portinha/ec.gif |
| .ee | Estónia | Estonia | http://www.gregoriano.org.br/portinha/ee.gif |
| .eg | Egito | Egypt | http://www.gregoriano.org.br/portinha/eg.gif |
| .eh | Saara Ocidental | Western Sahara | http://3.bp.blogspot.com/_5wS75p7WKLg/TN89fQSjKwI/AAAAAAAAA-c/hONtVAn0w4Q/s1600/800px-Flag_of_Western_Sahara.svg.png |
| .er | Eritreia | Eritrea | http://www.gregoriano.org.br/portinha/er.gif |
| .es | Espanha | Spain | http://www.gregoriano.org.br/portinha/es.gif |
| .et | Etiópia | Ethiopia | http://www.gregoriano.org.br/portinha/et.gif |
| .eu | Europa |  | http://4.bp.blogspot.com/_zjmToMJd6Ik/S9xj4GplEwI/AAAAAAAAADc/WtvjI90q7C8/s1600/bandeira20ue.jpg |
| .fi | Filândia | Finland | http://www.gregoriano.org.br/portinha/fi.gif |
| .fj | Fiji | Fiji | http://www.gregoriano.org.br/portinha/fj.gif |
| .fk | Ilhas Falkland (Malvinas) | Falkland Islands (Malvinas) | http://www.gregoriano.org.br/portinha/fk.gif |
| .fm | Estados Federativos da Micronésia | Micronesia | http://www.gregoriano.org.br/portinha/fm.gif |
| .fo | Ilhas Feroé | Faroe Islands | http://www.gregoriano.org.br/portinha/fo.gif |
| .fr | França | France | http://www.gregoriano.org.br/portinha/fr.gif |
| .fx | França Metropolitana | France, Metropolitan | http://www.gregoriano.org.br/portinha/fr.gif |
| .ga | Gabão | Gabon | http://www.gregoriano.org.br/portinha/ga.gif |
| .gb | Reino Unido  (o mais utilizado é .uk) | United Kingdom | http://www.gregoriano.org.br/portinha/gb.gif |
| .gd | Granada | Grenada | http://www.gregoriano.org.br/portinha/gd.gif |
| .ge | Geórgia | Georgia | http://www.gregoriano.org.br/portinha/ge.gif |
| .gf | Guiana Francesa | French Guiana | http://www.gregoriano.org.br/portinha/gf.gif |
| .gg | Ilhas Guernsey | Guersey Islands | http://www.gregoriano.org.br/portinha/gue.gif |
| .gh | Gana | Ghana | http://www.gregoriano.org.br/portinha/gh.gif |
| .gi | Gilbraltar | Gilbraltar | http://www.gregoriano.org.br/portinha/gi.gif |
| .gl | Gronelândia | Greenland | http://www.gregoriano.org.br/portinha/gl.gif |
| .gm | Gâmbia | Gambia | http://www.gregoriano.org.br/portinha/gm.gif |
| .gn | Guiné | Guinea | http://www.gregoriano.org.br/portinha/gf.gif |
| .gp | Guadalupe | Guadeloupe | http://www.gregoriano.org.br/portinha/gp.gif |
| .gq | Guiné Equatorial | Equatorial Guinea | http://www.gregoriano.org.br/portinha/gq.gif |
| .gr | Grécia | Greece | http://www.gregoriano.org.br/portinha/gr.gif |
| .gs | Ilhas Geórgia do Sul e Sandwich do Sul | South Georgia and the South Sandwich Islands | http://www.gregoriano.org.br/portinha/gs.gif |
| .gt | Guatemala | Guatemala | http://www.gregoriano.org.br/portinha/gt.gif |
| .gu | Guam | Guam | http://www.gregoriano.org.br/portinha/gu.gif |
| .gw | Guiné-Bissau | Guinea-Bissau | http://www.gregoriano.org.br/portinha/gw.gif |
| .gy | Guiana | Guyana | http://www.gregoriano.org.br/portinha/gy.gif |
| .hk | Hong Kong | Hong Kong | http://www.gregoriano.org.br/portinha/hk.gif |
| .hm | Ilhas Heard e Ilhas McDonald | Heard and McDonald Islands | http://www.gregoriano.org.br/portinha/hm.gif |
| .hn | Honduras | Honduras | http://www.gregoriano.org.br/portinha/hn.gif |
| .hr | Croácia | Croatia (Hrvatska) | http://www.gregoriano.org.br/portinha/hr.gif |
| .ht | Haiti | Haiti | http://www.gregoriano.org.br/portinha/ht.gif |
| .hu | Hungria | Hungary | http://www.gregoriano.org.br/portinha/hu.gif |
| .id | Indonésia | Indonesia | http://www.gregoriano.org.br/portinha/id.gif |
| .ie | Irlanda | Ireland | http://www.gregoriano.org.br/portinha/ie.gif |
| .il | Israel | Israel | http://www.gregoriano.org.br/portinha/il.gif |
| .im | Ilhas de Man |  | http://www.gregoriano.org.br/portinha/man.gif |
| .in | Índia | India | http://www.gregoriano.org.br/portinha/in.gif |
| .io | Território Britânico do Oceano Índico | British Indian Ocean Territory | http://upload.wikimedia.org/wikipedia/commons/thumb/6/6e/Flag_of_the_British_Indian_Ocean_Territory.svg/400px-Flag_of_the_British_Indian_Ocean_Territory.svg.png |
| .iq | Iraque | Iraq | http://www.gregoriano.org.br/portinha/iq.gif |
| .ir | Iran | Iran | http://www.gregoriano.org.br/portinha/ir.gif |
| .is | Islândia | Iceland | http://www.gregoriano.org.br/portinha/is.gif |
| .it | Itália | Italy | http://www.gregoriano.org.br/portinha/it.gif |
| .je | Ilhas Jersey | Jersey Islands | http://www.gregoriano.org.br/portinha/jer.gif |
| .jm | Jamaica | Jamaica | http://www.gregoriano.org.br/portinha/jm.gif |
| .jo | Jordânia | Jordan | http://www.gregoriano.org.br/portinha/jo.gif |
| .jp | Japão | Japan | http://www.gregoriano.org.br/portinha/jp.gif |
| .ke | Quénia | Kenya | http://www.gregoriano.org.br/portinha/ke.gif |
| .kg | Quirguistão | Kyrgyzstan | http://www.gregoriano.org.br/portinha/kg.gif |
| .kh | Camboja | Cambodia | http://www.gregoriano.org.br/portinha/kh.gif |
| .ki | Kiribati | Kiribati | http://www.gregoriano.org.br/portinha/ki.gif |
| .km | Comoros | Comoros | http://www.gregoriano.org.br/portinha/km.gif |
| .kn | Saint Kitts e Nevis | Saint Kitts and Nevis | http://www.gregoriano.org.br/portinha/kn.gif |
| .kp | Coréia do Norte | Korea (North) | http://www.gregoriano.org.br/portinha/kp.gif |
| .kr | Coréia do Sul | Korea | http://www.gregoriano.org.br/portinha/kr.gif |
| .kw | Kuwait | Kuwait | http://www.gregoriano.org.br/portinha/kw.gif |
| .ky | Ilhas Caiman | Cayman Islands | http://www.gregoriano.org.br/portinha/ky.gif |
| .kz | Cazaquistão | Kazakhstan | http://www.gregoriano.org.br/portinha/kz.gif |
| .la | Laos | Laos | http://www.gregoriano.org.br/portinha/la.gif |
| .lb | Líbano | Lebanon | http://www.gregoriano.org.br/portinha/lb.gif |
| .lc | Santa Lúcia | Saint Lucia | http://www.gregoriano.org.br/portinha/lc.gif |
| .li | Liechtenstein | Liechenstein | http://www.gregoriano.org.br/portinha/li.gif |
| .lk | Sri Lanka | Sri Lanka | http://www.gregoriano.org.br/portinha/lk.gif |
| .lr | Libéria | Liberia | http://www.gregoriano.org.br/portinha/lr.gif |
| .ls | Lasoto | Lesotho | http://www.gregoriano.org.br/portinha/ls.gif |
| .lt | Lituânia | Lithuania | http://www.gregoriano.org.br/portinha/lt.gif |
| .lu | Luxemburgo | Luxemburgo | http://www.gregoriano.org.br/portinha/lu.gif |
| .lv | Letónia | Latvia | http://www.gregoriano.org.br/portinha/lv.gif |
| .ly | Líbia | Libya | http://www.gregoriano.org.br/portinha/ly.gif |
| .ma | Marrocos | Morocco | http://www.gregoriano.org.br/portinha/ma.gif |
| .mc | Mónaco | Monaco | http://www.gregoriano.org.br/portinha/mc.gif |
| .md | Moldávia | Moldova | http://www.gregoriano.org.br/portinha/md.gif |
| .me | Montenegro |  | Ficheiro:Flag of Montenegro.svg |
| .mg | Madagáscar | Madagascar | http://www.gregoriano.org.br/portinha/mg.gif |
| .mh | Ilhas Marshall | Marshall Islands | http://www.gregoriano.org.br/portinha/mh.gif |
| .mk | Macedônia | Macedonia | http://www.gregoriano.org.br/portinha/mk.gif |
| .ml | Mali | Mali | http://www.gregoriano.org.br/portinha/ml.gif |
| .mm | Myanmar | Myanmar | http://www.gregoriano.org.br/portinha/mm.gif |
| .mn | Mongólia | Mongolia | http://www.gregoriano.org.br/portinha/mn.gif |
| .mo | Macau | Macau | http://www.gregoriano.org.br/portinha/mo.gif |
| .mp | Ilhas Marianas Nordeste | Northern Mariana Islands | http://www.gregoriano.org.br/portinha/mp.gif |
| .mq | Martinica | Martinique | http://www.gregoriano.org.br/portinha/mq.gif |
| .mr | Mauritânia | Mauritania | http://www.gregoriano.org.br/portinha/mr.gif |
| .ms | Montserrat | Montserrat | http://www.gregoriano.org.br/portinha/ms.gif |
| .mt | Malta | Malta | http://www.gregoriano.org.br/portinha/mt.gif |
| .mu | Maurício | Mauritius | http://www.gregoriano.org.br/portinha/mu.gif |
| .mv | Maldivas | Maldives | http://www.gregoriano.org.br/portinha/mv.gif |
| .mw | Malawi | Malawi | http://www.gregoriano.org.br/portinha/mw.gif |
| .mx | México | Mexico | http://www.gregoriano.org.br/portinha/mx.gif |
| .my | Malásia | Malaysia | http://www.gregoriano.org.br/portinha/my.gif |
| .mz | Moçambique | Mozambique | http://www.gregoriano.org.br/portinha/mz.gif |
| .na | Namíbia | Namibia | http://www.gregoriano.org.br/portinha/na.gif |
| .nc | Nova Calédonia | New Caledonia | http://www.gregoriano.org.br/portinha/nc.gif |
| .ne | Níger | Niger | http://www.gregoriano.org.br/portinha/ne.gif |
| .nf | Ilhas Norfolk | Norfolk Island | http://www.gregoriano.org.br/portinha/nf.gif |
| .ng | Nigéria | Nigeria | http://www.gregoriano.org.br/portinha/ng.gif |
| .ni | Nicarágua | Nicaragua | http://www.gregoriano.org.br/portinha/ni.gif |
| .nl | Holanda (Países Baixos) | Netherlands | http://www.gregoriano.org.br/portinha/nl.gif |
| .no | Noruega | Norway | http://www.gregoriano.org.br/portinha/no.gif |
| .np | Nepal | Nepal | http://www.gregoriano.org.br/portinha/np.gif |
| .nr | Nauru | Nauru | http://www.gregoriano.org.br/portinha/nr.gif |
| .nu | Niue | Niue | http://www.gregoriano.org.br/portinha/nu.gif |
| .nz | Nova Zelândia | New Zealand | http://www.gregoriano.org.br/portinha/nz.gif |
| .om | Omã | Oman | http://www.gregoriano.org.br/portinha/om.gif |
| .pa | Panamá | Panama | http://www.gregoriano.org.br/portinha/pa.gif |
| .pe | Peru | Peru | http://www.gregoriano.org.br/portinha/pe.gif |
| .pf | Polinésia Francesa | French Polynesia | http://www.gregoriano.org.br/portinha/pf.gif |
| .pg | Papua – Nova Guiné | Papua New Guinea | http://www.gregoriano.org.br/portinha/pg.gif |
| .ph | Filipinas | Philippines | http://www.gregoriano.org.br/portinha/ph.gif |
| .pk | Paquistão | Pakistan | http://www.gregoriano.org.br/portinha/pk.gif |
| .pl | Polónia | Poland | http://www.gregoriano.org.br/portinha/pl.gif |
| .pm | Saint Pierre e Miquelon | St. Pierre and Miquelon | http://www.gregoriano.org.br/portinha/pm.gif |
| .pn | Pitcaim | Pitcaim | http://www.gregoriano.org.br/portinha/pn.gif |
| .pr | Porto Rico | Puerto Rico | http://www.gregoriano.org.br/portinha/pr.gif |
| .ps | Palestina | Palestina | http://upload.wikimedia.org/wikipedia/commons/thumb/0/00/Flag_of_Palestine.svg/250px-Flag_of_Palestine.svg.png |
| .pt | Portugal | Portugal | http://www.gregoriano.org.br/portinha/pt.gif |
| .pw | Palau | Palau | http://www.gregoriano.org.br/portinha/pw.gif |
| .py | Paraguai | Paraguay | http://www.gregoriano.org.br/portinha/py.gif |
| .qa | Qatar | Qatar | http://www.gregoriano.org.br/portinha/qa.gif |
| .re | Reunião | Reunion | http://www.gregoriano.org.br/portinha/re.gif |
| .ro | Roménia | Romania | http://www.gregoriano.org.br/portinha/ro.gif |
| .ru | Rússia | Russian Federation | http://www.gregoriano.org.br/portinha/ru.gif |
| .rw | Ruanda | Rwanda | http://www.gregoriano.org.br/portinha/rw.gif |
| .sa | Arábia Saudita | Saudi Arabia | http://www.gregoriano.org.br/portinha/sa.gif |
| .sb | Ilhas Salomão | Solomon Islands | http://www.gregoriano.org.br/portinha/sb.gif |
| .sc | Seychelles | Seychelles | http://www.gregoriano.org.br/portinha/sc.gif |
| .sd | Sudão | Sudan | http://www.gregoriano.org.br/portinha/sd.gif |
| .se | Suécia | Sweden | http://www.gregoriano.org.br/portinha/se.gif |
| .sg | Singapura | Singapore | http://www.gregoriano.org.br/portinha/sg.gif |
| .sh | Santa Helena | St. Helena | http://www.gregoriano.org.br/portinha/sh.gif |
| .si | Eslovénia | Slovenia | http://www.gregoriano.org.br/portinha/si.gif |
| .sj | Ilhas Svalbard e Jan Mayen | Svalbard and Jan Mayen | http://www.gregoriano.org.br/portinha/sj.gif |
| .sk | Eslováquia | Slovak Republic | http://www.gregoriano.org.br/portinha/sk.gif |
| .sl | Serra Leoa | Sierra Leone | http://www.gregoriano.org.br/portinha/sl.gif |
| .sm | San Marino | San Marino | http://www.gregoriano.org.br/portinha/sm.gif |
| .sn | Senegal | Senegal | http://www.gregoriano.org.br/portinha/sn.gif |
| .so | Somália | Somalia | http://www.gregoriano.org.br/portinha/so.gif |
| .sr | Suriname | Suriname | http://www.gregoriano.org.br/portinha/sr.gif |
| .ss | Sudão do Sul | South Sudan | Bandeira do Sudão do Sul |
| .st | São Tomé e Príncipe | Sao Tome and Principe | http://www.gregoriano.org.br/portinha/st.gif |
| .su | União Soviética |  | Bandeira da União Soviética |
| .sv | El Salvador | El Salvador | http://www.gregoriano.org.br/portinha/sv.gif |
| .sy | Síria | Syria | http://www.gregoriano.org.br/portinha/sy.gif |
| .sz | Suazilândia | Swaziland | http://www.gregoriano.org.br/portinha/sz.gif |
| .tc | Ilhas Turcas e Caicos | Turks and Caicos Islands | http://www.gregoriano.org.br/portinha/tc.gif |
| .td | Chade | Chad | http://www.gregoriano.org.br/portinha/td.gif |
| .tf | Terras Antárticas e Francesas | French Southern Territories | Bandeira |
| .tg | Tago | Togo | http://www.gregoriano.org.br/portinha/tg.gif |
| .th | Tailândia | Thailand | http://www.gregoriano.org.br/portinha/th.gif |
| .tj | Tajiquistão | Tajikistan | http://www.gregoriano.org.br/portinha/tj.gif |
| .tk | Tokelau | Tokelau | http://www.gregoriano.org.br/portinha/tk.gif |
| .tm | Turcomênia | Turkmenistan | http://www.gregoriano.org.br/portinha/tm.gif |
| .tn | Tunísia | Tunisa | http://www.gregoriano.org.br/portinha/tn.gif |
| .to | Tonga | Tonga | http://www.gregoriano.org.br/portinha/to.gif |
| .tp | Timor Leste | East Timor | http://www.gregoriano.org.br/portinha/tl.gif |
| .tr | Turquia | Turkey | http://www.gregoriano.org.br/portinha/tr.gif |
| .tt | Trindad e Tobago | Trindad and Tobago | http://www.gregoriano.org.br/portinha/tt.gif |
| .tv | Tuvalu | Tuvalu | http://www.gregoriano.org.br/portinha/tv.gif |
| .tw | Taiwan | Taiwan | http://www.gregoriano.org.br/portinha/tw.gif |
| .tz | Tanzânia | Tanzania | http://www.gregoriano.org.br/portinha/tz.gif |
| .ua | Ucrânia | Ukraine | http://www.gregoriano.org.br/portinha/ua.gif |
| .ug | Uganda | Ugana | http://www.gregoriano.org.br/portinha/ug.gif |
| .uk | Reino Unido (Inglaterra) | United Kingdom | http://www.gregoriano.org.br/portinha/gb.gif |
| .um | Ilhas Menores e Distantes dos Estados Unidos | United States Minor Outlying Islands | http://www.gregoriano.org.br/portinha/us.gif |
| .us | Estados Unidos | United States | http://www.gregoriano.org.br/portinha/us.gif |
| .uy | Uruguai | Uruguay | http://www.gregoriano.org.br/portinha/uy.gif |
| .uz | Uzbequistão | Uzbekistan | http://www.gregoriano.org.br/portinha/uz.gif |
| .va | Vaticano | Vatican City State | http://www.gregoriano.org.br/portinha/va.gif |
| .vc | São Vicente e Granadinas | Saint Vicent and the Grenadines | Bandeira de São Vicente e Granadinas |
| .ve | Venezuela | Venezuela | http://www.gregoriano.org.br/portinha/ve.gif |
| .vg | Ilhas Virgens Britânicas | Virgin Islands (Britsh) | http://www.gregoriano.org.br/portinha/vg.gif |
| .vi | Ilhas Virgens Americanas | Virgin Islands (United States) | http://www.gregoriano.org.br/portinha/vi.gif |
| .vn | Vietnam | Viet Nam | http://www.gregoriano.org.br/portinha/vn.gif |
| .vu | Vanuatu | Vanuatu | http://www.gregoriano.org.br/portinha/vu.gif |
| .wf | Ilhas Wallis e Futuna | Wallis and Futuna Islands | http://www.gregoriano.org.br/portinha/wf.gif |
| .ws | Samoa | Samoa | http://www.gregoriano.org.br/portinha/ws.gif |
| .ye | Iémen | Yemen | http://www.gregoriano.org.br/portinha/ye.gif |
| .yt | Mayotte | Mayotte | http://www.gregoriano.org.br/portinha/yt.gif |
| .yu | Iugoslávia (Sérvia) | Yugoslavia | http://upload.wikimedia.org/wikipedia/commons/thumb/e/e7/Flag_of_the_Kingdom_of_Yugoslavia.svg/250px-Flag_of_the_Kingdom_of_Yugoslavia.svg.png |
| .za | África do Sul | South Africa | http://www.gregoriano.org.br/portinha/za.gif |
| .zm | Zâmbia | Zambia | http://www.gregoriano.org.br/portinha/zm.gif |
| .zr | Zaire | Zaire | Flag |
| .zw | Zimbabwe | Zimbabwe | http://www.gregoriano.org.br/portinha/zw.gif |

Tabela 02 – Rótulos de domínios de Paises

**3.3 – Domínio Inverso**

O **Domínio Inverso** é utilizado para mapear endereços IP em um nome. Este tipo de consulta é chamado de consulta inversa ou de **Ponteiro (PTR)**. Em uma consulta inversa é adicionado ao espaço de nomes de domínio com um nó de primeiro nível chamado arpa (por motivos históricos), também é adicionado um segundo nível chamado in-addr (de inverse address – endereço inverso), o restante é definido pelo endereço IP.

Os servidores que manipulam domínios inversos também são hierárquicos, com isso, a parte de **netid** do endereço deve estar em um nível mais alto que a **subnetid** que por sua vez está em um nível mais alto que o **hostid**. Essa configuração faz o domínio parecer invertido, quando comparado com um domínio genérico ou de país.

Vamos a um exemplo de consulta inversa com a ferramenta ***nslookup***:

root@fusion:~# nslookup 192.185.209.214

Server: 192.168.5.2

Address: 192.168.5.2#53

Non-authoritative answer:

214.209.185.192.in-addr.arpa name = br160-ip11.hostgator.com.br.

Authoritative answers can be found from:

185.192.in-addr.arpa nameserver = ns1.p13.dynect.net.

185.192.in-addr.arpa nameserver = ns4.p13.dynect.net.

185.192.in-addr.arpa nameserver = ns2.p13.dynect.net.

185.192.in-addr.arpa nameserver = ns3.p13.dynect.net.

root@fusion:~#

Como podemos observar o endereço IP 192.185.209.214 (escolhido aleatoriamente) em uma consulta inversa, foi resolvido com o nome **br160-ip11.hostgator.com.br.**

A figura abaixo ilustra a configuração do domínio inverso.

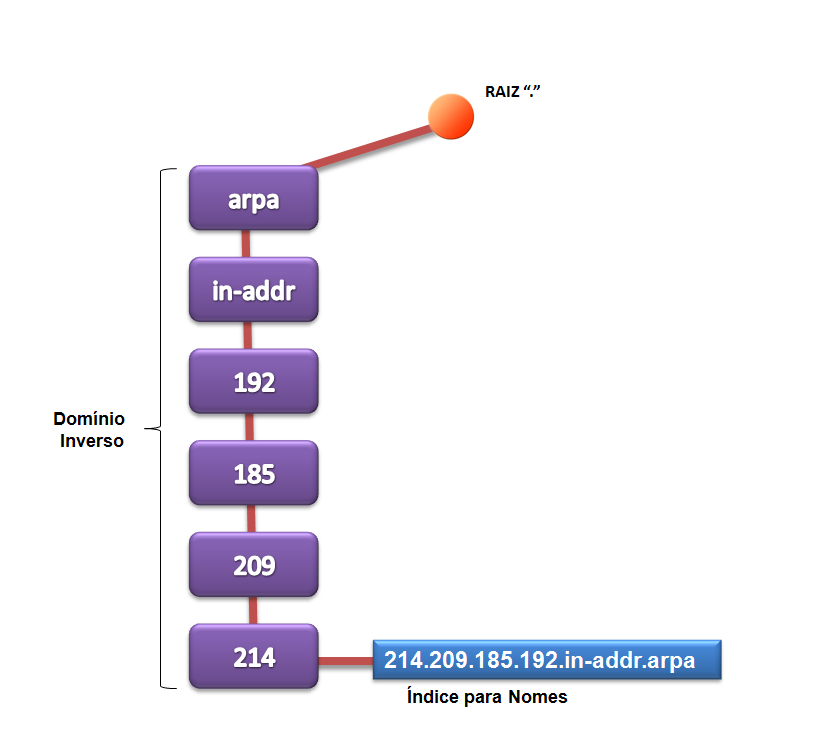


Figura 01 – Configuração do Domínio Inverso

**4 – Resolução de Nomes DNS**

O **DNS** faz o mapeamento de um nome para endereço IP ou de um endereço IP para nome, a isso se dá o nome de resolução de nome/endereço.

**4.1 – Resolver**

O DNS é um aplicativo cliente-servidor. Quando um host necessita resolver um nome para endereço IP, ele chama um cliente DNS denominado **Resolver**.

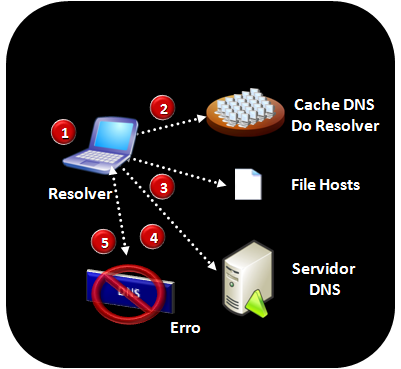


Figura 01 - Resolver

Quando um aplicativo necessita resolver um nome para endereço IP (ou vice-versa), esse aplicativo passar a consulta para o **Resolver**, que inicialmente tentará resolver usando recursos locais como o **Cache DNS** ou o arquivo **Hosts**. Caso não obtiver a resposta será encaminhado para o **Servidor DNS** primário configurado no cliente.

As etapas a seguir demonstram como ficaria a resolução do nome no **Resolver** (como ilustrado na **Figura 01**):

1. **Resolver** 🡪 Ao solicitar a resolução de um endereço o processo de resolução é iniciado.
2. **Cache DNS** 🡪 Todas as solicitações feitas para o **Servidor DNS** com sucesso são mantidos na memória local do host por um tempo. O primeiro lugar a ser consultado todas as vezes em que um endereço for passado para o **Resolver** é o **Cache DNS** local do host.
3. **Arquivo Hosts 🡪** Se não for encontrado uma resposta para a consulta no **Cache DNS**, o **Resolver** irá consultar o arquivo **Hosts**, o qual é um arquivo texto com o mapeamento nome endereço.
4. **Servidor DNS Preferencial 🡪** Se mesmo assim não houver resposta, o **Resolver** irá enviar a consulta para o **Servidor Primário**.
5. **OK ou Erro 🡪** Depois que o **Resolver** receber a resposta, ele interpreta e vê se é uma solução real ou um erro e, finalmente envia o resultado para o processo que o solicitou.

**4.1.1 – Cache DNS Local**

Todas as vezes que um nome é resolvido às informações são armazenadas no **Cache DNS Local**, e são mantidos na memória para agilizar o processo de resolução de nome. As vezes necessitamos limpar esse **Cache DNS Local** por conter informações incorretas gravadas. Para isso podemos utilizar algumas ferramentas que iremos ver a seguir.

Na família **Microsoft** pode consultar seu **Cache DNS Local** com o comando ***ipconfig*** no Prompt de Comando desta forma:

C:\Users\w3ll>ipconfig /displaydns

Configuração de IP do Windows

www.googleadservices.com

----------------------------------------

Nome do Registro. . . . . . . . . . . . . : www.googleadservices.com

Tipo de Registro. . . . . . . . . . . . . : 1

Tempo de Vida . . . . . . . . . . . . . . : 7019

Comprimento dos Dados . . . . . . . . . . : 4

Seção. . . . . . . . . . . . . . . . . . . : Resposta

Registro (Host). . . . . . . . . . . . . . : 173.194.118.249

--==[ Resumido ]==--

Nome do Registro. . . . . . . . . . . . . : gpush.cogocast.net

Tipo de Registro. . . . . . . . . . . . . : 1

Tempo de Vida . . . . . . . . . . . . . . : 343

Comprimento dos Dados . . . . . . . . . . : 4

Seção. . . . . . . . . . . . . . . . . . . : Resposta

Registro (Host). . . . . . . . . . . . . . : 208.118.234.100

Nome do Registro. . . . . . . . . . . . . : gpush.cogocast.net

Tipo de Registro. . . . . . . . . . . . . : 1

Tempo de Vida . . . . . . . . . . . . . . : 343

Comprimento dos Dados . . . . . . . . . . : 4

Seção. . . . . . . . . . . . . . . . . . . : Resposta

Registro (Host). . . . . . . . . . . . . . : 208.118.234.120

C:\Users\w3ll>

E para limpar o **Cache DNS Local** com o mesmo comando podemos fazer assim:

C:\Users\w3ll>ipconfig /flushdns

Configuração de IP do Windows

Liberação do Cache do DNS Resolver bem-sucedida.

C:\Users\w3ll>

Já na família **UNIX-Like**, não é feito **Cache DNS Local** por padrão, sendo necessária a instalação de um utilitário o **NSCD**. Após a instalação devemos entrar no arquivo de configuração do utilitário e habilitar o **Cache DNS Local**, o arquivo fica em ***/etc/nscd.conf***, vamos a pratica:

root@fusion:~# aptitude install nscd

The following NEW packages will be installed:

nscd

0 packages upgraded, 1 newly installed, 0 to remove and 4 not upgraded.

Need to get 0 B/211 kB of archives. After unpacking 344 kB will be used.

Selecting previously unselected package nscd.

(Reading database ... 36197 files and directories currently installed.)

Unpacking nscd (from .../nscd\_2.13-38+deb7u3\_i386.deb) ...

Processing triggers for man-db ...

Setting up nscd (2.13-38+deb7u3) ...

Starting Name Service Cache Daemon: nscd.

root@fusion:~# vi /etc/nscd.conf

--==[ Resumido ]==--

logfile /var/log/nscd.log

debug-level 0

enable-cache passwd no

enable-cache hosts yes

enable-cache group no

enable-cache services no

--==[ Resumido ]==--

"/etc/nscd.conf" 79L, 2147C written

root@fusion:~# /etc/init.d/nscd restart

Restarting Name Service Cache Daemon: nscd.

root@fusion:~#

**Observação:** Por questões de segurança, estou desabilitando os outros caches como o de senhas, grupos e serviços.

Infelizmente não temos um comando para nos mostrar os registros do **Cache DNS Local** no **UNIX-Like**, mas podemos ver as entradas no arquivo de log que fica em ***/var/log/nscd.log*** e os arquivos de cache ficam em ***/var/cache/nscd/hosts***.

Para limpar o **Cache DNS Local** do **NSCD** basta reinicia-lo como demonstrado anteriormente após a configuração do arquivo ***nscd.conf***.

Podemos gerar estatísticas com o comando nscd -g.

root@fusion:~# nscd -g

nscd configuration:

5 server debug level

5m 44s server runtime

4 current number of threads

32 maximum number of threads

0 number of times clients had to wait

no paranoia mode enabled

3600 restart internal

5 reload count

--==[ Resumido ]==--

hosts cache:

yes cache is enabled

yes cache is persistent

yes cache is shared

211 suggested size

216064 total data pool size

456 used data pool size

3600 seconds time to live for positive entries

20 seconds time to live for negative entries

0 cache hits on positive entries

0 cache hits on negative entries

6 cache misses on positive entries

0 cache misses on negative entries

0% cache hit rate

3 current number of cached values

3 maximum number of cached values

0 maximum chain length searched

0 number of delays on rdlock

0 number of delays on wrlock

0 memory allocations failed

yes check /etc/hosts for changes

--==[ Resumido ]==--

root@fusion:~#

**4.1.2 – Arquivo Hosts**

O arquivo Hosts é um arquivo texto que contém os registros de nome de host para IP. Ele é utilizado para fazer um mapeamento local. No **Windows** ele está localizado em ***%systemroot%\system32\drivers\etc\*** e no **Linux** fica em ***/etc/hosts***. Observe as entradas no Linux:

root@fusion:~# cat /etc/hosts

127.0.0.1 localhost

127.0.1.1 fusion.how2security.com.br fusion

# The following lines are desirable for IPv6 capable hosts

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

root@fusion:~#

Ou no Windows.

C:\Users\w3ll>type %systemroot%\system32\drivers\etc\hosts

# Copyright (c) 1993-2009 Microsoft Corp.

#

# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

#

# This file contains the mappings of IP addresses to host names. Each

# entry should be kept on an individual line. The IP address should

# be placed in the first column followed by the corresponding host name.

# The IP address and the host name should be separated by at least one

# space.

#

# Additionally, comments (such as these) may be inserted on individual

# lines or following the machine name denoted by a '#' symbol.

#

# For example:

#

# 102.54.94.97 rhino.acme.com # source server

# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.

# 127.0.0.1 localhost

# ::1 localhost

C:\Users\w3ll>

**4.2 – Resolução Recursiva**

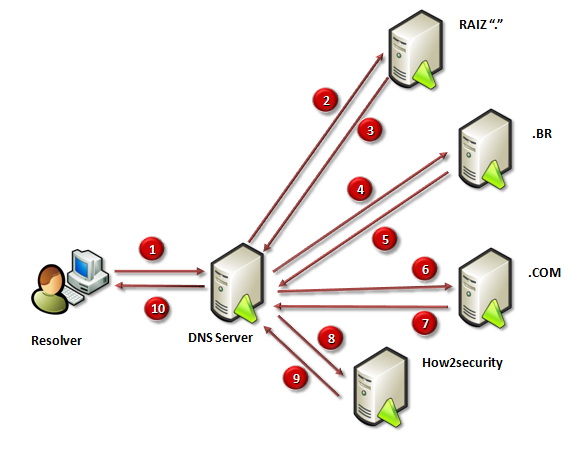


Figura 02 – Resolução Recursiva

A Resolução Recursiva irá utilizar a hierarquia DNS para entregar a resposta final para o **Resolver** **(Cliente DNS)**. Desta forma o Servidor irá consultar desde servidores raízes até os servidores que tem autoridade sobre o domínio.

O **Servidor DNS** poderá responder o **Resolver** com uma das seguintes respostas:

* **An Authoritative Answer (Resposta com Autoridade)** 🡪 Este tipo de resposta é obtido quando o nome é resolvido diretamente pelo **Servidor DNS** que é a autoridade para o domínio pesquisado.
* **A Positive Answer (Resposta Positiva)** 🡪 É uma resposta com o resultado para o nome pesquisado ou informações associadas ao nome são retornadas para o **Resolver**.
* **A Referral Answer (Uma Referência)** 🡪 É uma referência a recursos ou outros **Servidores DNS** que podem ser utilizados para a resolução do nome. Este tipo de resposta é enviado no caso do **Servidor DNS** não suportar o método de recursão.
* **A Negative Answer (Uma Resposta Negativa)** 🡪 É uma resposta indicando que houve algum erro, seja ele, o recurso não existe, ou ainda o recurso existe porém o tipo de registro não confere (Para maiores informações olhe a **Tabela 00 - Mensagens DNS**).

As etapas a seguir demonstram como ficaria a **Resolução do Nome Recursivo** (como ilustrado na **Figura 02**):

1. O **Resolver** envia uma consulta recursiva para o **Servidor DNS** Preferencial para resolver o nome ***www.how2security.com.br***.
2. O **Servidor DNS** retira o nome do recurso (no nosso caso o ***www***, que é o nome do host a ser pesquisado), então o **Servidor DNS** envia uma **Consulta Iterativamente** para um dos **Servidores Raiz** (root hits) para saber quem é a autoridade para o domínio pesquisado.
3. O **Servidor Raiz** responde com uma referência para os servidores responsável pelos domínios ***.br***.
4. O **Servidor DNS** envia uma **Consulta Iterativa** para os **Servidor DNS** com autoridade para o domínio ***.br*** se ele sabe quem é a autoridade para o domínio ***how2security.com.br***.
5. O **Servidor com Autoridade** para o domínio ***.br*** responde com uma referência para os servidor responsável pelo domínio ***.com.br***.
6. O **Servidor DNS** envia uma **Consulta Iterativa** para os **Servidor DNS** com autoridade para o domínio ***.com.br*** se ele sabe quem é a autoridade para o domínio ***how2security.com.br***.
7. O **Servidor com Autoridade** para o domínio ***.com.br*** responde com o endereço IP do **Servidor DNS** com autoridade para o domínio ***.how2security.com.br***.
8. O **Servidor DNS** envia uma Consulta para os **Servidor DNS** com autoridade para o domínio ***.how2security.com.br***, perguntando quem é o recurso [***www.how2security.com.br***](http://www.how2security.com.br).
9. O **Servidor DNS** com autoridade para o domínio **.how2security.com.br** recebe a consulta para resolver o nome do recurso **www**. Como este servidor é a autoridade para o domínio, ele pesquisa em sua zona, encontrando o registro ele envia o **Endereço IP** do host **www** como resposta. O **Servidor DNS** recebendo a resposta, faz uma cópia desta resposta no **Cache DNS** e retorna para o **Resolver** que originou a consulta.
10. O **Resolver** recebe o resultado da consulta, grava a resposta no **Cache DNS Local** e, finalmente envia o resultado para o processo que o solicitou.

**4.3 – Resolução Iterativa**

O processo de iteração é utilizado entre o **Resolver** e um ou mais **Servidores DNS**. A Resolução Iterativa pode ocorrer caso:

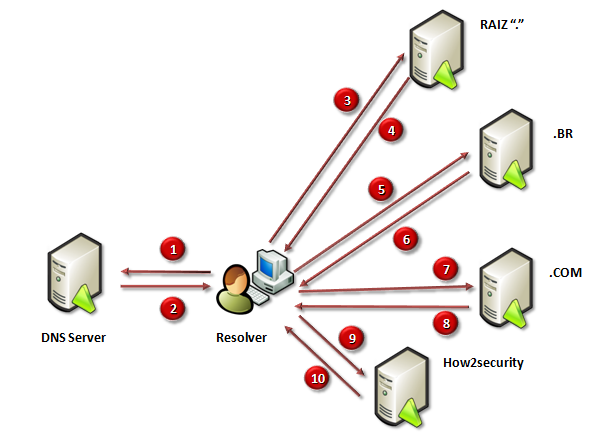


Figura 03 – Resolução Iterativa

* O **Resolver** tenta utilizar o processo de **Recursão**, mas a **Recursão** está desabilitada no **Servidor DNS**;
* O **Resolver** não solicitou uso de **Recursão** ao pesquisar o **Servidor DNS**;
* O **Resolver** faz uma consulta ao **Servidor DNS**, informando que é esperada a melhor resposta que o **Servidor DNS** puder fornecer imediatamente, sem consultar outros **Servidores DNS**.

O processo de **Resolução Iterativa**, o **Resolver** envia uma consulta repetidamente até obter uma resposta positiva ou negativa. Se o **Servidor DNS** **Preferencial** do **Resolver** for a autoridade para o domínio consultado ele responde imediatamente, caso contrário o **Servidor DNS** enviará uma lista de outros Servidores que poderá resolver o nome do recurso. Então o **Resolver** continuará a perguntar até obter a resposta. No nosso exemplo (**Figura 03**) o **Resolver** consultou **5 Servidores DNS**.

**4.4 – Cache**

O trabalho básico do **Servidor DNS** é responder às consultas enviadas pelos clientes, quer seja utilizando **Recursão** ou **Iteração**. A medida que os nomes vão sendo resolvidos, esta informação fica armazenada no **Cache do Servidor DNS**. Com o uso do cache, futuras consultas à nomes já resolvidos, podem ser respondidas diretamente a partir do **Cache do Servidor DNS**, agiliza o processo de resolução de nomes e também reduz o tráfego de rede gerado pelo **DNS**.

Quando um **Resolve** obtém uma resposta do **Servidor DNS** através do **Cache**, o **Servidor DNS** marca a resposta como não **Autorizada**.

O **Cache** acelera a resolução, mas também pode ser problemático. Pois as informações podem está desatualizada e o mapeamento errado. Para evitar isso, são utilizadas duas técnicas.

A Primeira é o **Servidor Autorizado** sempre adicionar uma informação no mapeamento, chamada de tempo de vida (**Time-To-Live -TTL**). Esta informação determina quanto tempo a informação será mantida no **Cache** até ser descartada. O Segundo o **Servidor DNS** exige que cada Servidor mantenha um contador de **TTL** para cada mapeamento colocado no **Cache**. Dessa forma a memória **Cache** é pesquisada periodicamente, e seus mapeamentos com **TTL** expirados devem ser eliminados**.**

**5 – Arquivo de Zona do DNS**

Os arquivos de transferência do **DNS** são mantidos em formato texto para facilitar a edição pelos sistemas mantenedores. Estes arquivos não são transmitidos a outros servidores, pois para isso existem protocolos de transferências. Eles servem para facilitar a manutenção dos **Servidores DNS** e segue um padrão de escrita.

**5.1 – Arquivo Master**

O arquivo **Master** é um arquivo de texto que contem **Resource Records**, organizado por linhas simples, ou seja, cada linha tem um **Resource Record (RR)**. Definido em sua maior parte na seção 5 da **RFC 1035**, possibilita a definição de zonas DNS para domínios além de poder ser usado para listagem de conteúdo de cache.

Este arquivo possui uma sequência de entradas orientadas por linha que se referem aos **RRs** com diversos campos separados por qualquer combinação de espaço em branco. **Tabs** também são tratados como espaço em branco.

Já as linhas em branco são ignoradas indicando que não existe um **RR** e podem ser colocadas em qualquer local do arquivo.

Comentários podem ser inseridos em qualquer linha, sendo no início da linha ou após o último campo de um **RR**.

Existem três diretivas de controle utilizadas, sendo elas **$ORIGIN**, **$INCLUDE** e **$TTL**.

**$ORIGIN** declara o nome de domínio para nomes relativos que não terminem com (**.**) ponto. Se não especificado, será utilizado o nome definido para a zona no software executando o serviço de **DNS**. Também temos o **$INCLUDE** que podemos carregar arquivos externos dentro do nosso arquivo **Master**. Ele é útil para carregarmos diversos arquivos de domínio contendo outros **RRs** . Por exemplo, se tivermos diversos domínios administrados por usuários diferentes, podemos criar um arquivo para cada um colocar seus **RR** e depois carregarmos cada configuração utilizando as diretivas **$INCLUDE**.

Um detalhe importante é que se tivermos uma entrada **$ORIGIN** em um arquivo incluído pelo **$INCLUDE**, este não altera o domínio relativo para o arquivo pai, apenas para os nomes relativos dentro do mesmo arquivo.

A sintaxe para estas duas entradas são:

***$ORIGIN <nome do domínio>***

***$INCLUDE <nome do arquivo> [<nome do domínio>]***

Já a diretiva **$TTL**, definida na **RFC 2308**, define o **TTL** **Padrão** da zona, o qual deverá ser usado por todos os **Resource Records** abaixo da diretiva que não tiverem o campo **TTL** declarado. Esta diretiva deve estar sempre presente e acima do primeiro **RR**. A sintaxe para esta é bem simples como pode ser vista abaixo:

***$TTL <TTL>***

Onde ***<TTL>*** é um número inteiro entre **0** e **2147483647** (2^31-1), vide **RFC 2181**.

As entradas de **Resource Records** podem ser definidas de duas formas, sendo elas***:<blank> <ResourceRecord>***  
***<owner-name> <ResourceRecord>***

No primeiro exemplo temos uma entrada que inicia com um espaço em branco (ou tab), o que assume que o nome do recurso (node) é o definido anteriormente ou o definido pela entrada **$ORIGIN**.

No segundo caso o nome é definido, podendo ser absoluto ou relativo. O nome do node é escrito com uma sequência de caracteres separados por (.) pontos. Quando terminado em ponto, indica que está expresso de forma absoluta, ou seja, desde a raíz de nomes o nome desejado. Por exemplo, para referenciarmos o domínio **how2lab.com.br** usaríamos algo como:

**host.how2lab.com.br.**

Se não colocarmos o ponto no final, será considerado um nome relativo (ao invés de absoluto) e será completado com o domínio definido em **$ORIGIN** ou na configuração da zona, ficando da seguinte forma:

**host** **para** **host.how2security.com.br**

Caso a intenção seja especificar um nome absoluto e que contenha um (.) no final, o domínio origem será adicionado, ficando algo como:

host.how2lab.com.br**.how2security.com.br**

Cada ***Resource Record <Resource Record>*** possui quatro campos, sendo dois campos opcionais, que são **TTL** e **CLASS**, e mais dois campos que definem o registro, **TYPE** e **RDATA**.

**TTL** define o tempo válido para cache de um determinado **RR**. Caso seja omitido, o valor padrão definido na diretiva **$TTL** será usado.

**CLASS** define a família de protocolos ou uma instância de protocolo do **RR**. Normalmente o valor definido é **IN**, que representa **“Internet Protocol”.**

Abaixo temos um formato genérico de um **Resource Record**:

**<owner-name> <ttl> <class> <type> <rdata>**

Pelo fato destes arquivos serem simples arquivos de texto, alguns codificadores são necessários para delimitação de cada recurso ou diretiva, como forma de organização e interpretação. Os principais são:

* **.** 🡪 Indica o nome do domínio atual.
* **@** 🡪 Declara a origem atual (o domínio definido em **$ORIGIN**).
* **..** 🡪 Representa o nome de uma raiz nula.
* **;** 🡪 Inicia um comentário na linha.
* **()** 🡪 Agrupa dados entre linhas seguidas. Utilizado para facilitar a visualização, geralmente usado no registro **SOA**.
* **\** 🡪 Considera o proximo caracter como literal, quando usarmos (.) ponto, ou (“) aspas. Por exemplo para definirmos o email **roberto.cruz** como responsável pelo domínio podemos usar ***roberto\.cruz.how2security.com.br***

Para que uma zona possa ser carregada com sucesso, algumas checagens devem ser feitas, por exemplo: Todos os **Resource Records** devem ser da mesma classe;

* Um registro **SOA** deve estar presente no início da zona, sendo o primeiro **RR**;
* Caso exista alguma delegação a mesma deve estar declarada.

**5.2 – Principais Tipos de Registros**

Existem diversos tipos diferentes de registros DNS disponíveis.

* **A - Address** **→** Mapeamento de nomes para endereços IPv4. Especifica um endereço IP direto;
* **AAAA - Address IPv6** **→** Mapeamento de nome para endereço IPv6. Especifica um endereço IPv6;
* **NS - NameServer** **→** Especifica servidores DNS para o domínio ou subdomínio;
* **CNAME - Canonical NAME** **→** Um apelido para outro hostname (**aliases**);
* **MX - Mail Exchanger** **→** O servidor de e-mail. O registro **MX** é seguido de um número que determina a prioridade do servidor. Quando menor o número, maior será a prioridade do servidor. A faixa de valores numéricos permitida é **0** - **65535**;
* **PTR - Pointer** → Mapeamento de endereços IP para nomes. Aponta o hostname/domínio reverso a partir de um endereço IP;
* **SOA - Start Of Authority** **→** Indica o responsável por respostas autoritativas por um domínio;
  + **@ - AT** **→** Define a localização deste domínio;
  + **Serial** **🡪** Serve para avisar aos servidores escravos sobre as atualizações do banco de dados. O servidor escravo pergunta periodicamente ao servidor mestre sobre o registro **SOA**. Se o número serial no registro **SOA** do servidor mestre for maior que o da cópia do arquivo de zona no escravo, este transfere toda zona do servidor mestre. De outra forma, o servidor escravo assume ter uma cópia igual e não procede com a transferência de zona. O número serial deve ser incrementado toda vez que o domínio for atualizado para manter o servidor escravo sincronizado com o mestre;
  + **Refresh** **→** Intervalo de tempo que o servidor escravo compara seu número serial com o número serial do servidor mestre;
  + **Retry** **→** Intervalo em que, caso o servidor mestre pare seu funcionamento, o servidor escravo tentará reatar a comunicação com o servidor mestre repetidamente;
  + **Expire** **→** Tempo de vida útil do banco de dados do domínio em um servidor escravo. Caso este tempo seja ultrapassado sem ser realizada uma conexão com o servidor mestre, os dados ali armazenados são considerados desatualizados. Em certos casos, o servidor poderá até parar de resolver nomes de DNS;
  + **Minimum (TTL - Time To Live)** **→** Valor mínimo de **TTL** que deve ser configurado em qualquer **RR** nesta zona;
* **TXT - Text** **→** Permite incluir um texto curto em um hostname; usado para implementar o **SPF**;
* **WKS - Well Know Services** **→** Serviços bem conhecidos;
* **HINFO - Host Information** **→** Informações sobre um computador;
* **SRV - Service** **→** Permite definir serviços disponíveis em um domínio.

Estes são os principais e que você provavelmente vai achar por aí. Vamos agora considerar alguns deles que requerem carinho especial dos administradores.

**5.3 – SOA**

O **SOA** ou **Start Of Authority** indica o servidor e administrador responsável por um domínio, além de indicar outras informações úteis, como número serial da zona DNS, tempo de vida do registro **SOA**, intervalo de replicação de zonas, etc.

Veja um exemplo:

ecosport:~# dig -t soa uol.com.br

...

;; ANSWER SECTION:

**(1)**uol.com.br. **(2)**3599 **(3)**IN **(4)**SOA **(5)**eliot.uol.com.br. root.uol.com.br. **(6)**2010032508 **(7)**7200 **(8)**3600 **(9)**432000 **(10)**3600

...

ecosport:~#

1. Nome da zona consultada;
2. TTL do registro na memória do seu DNS;
3. Tipo de registro;
4. DNS responsável pela zona;
5. E-mail do responsável pelo DNS acima;
6. Número serial da zona; recomenda-se o formato **YYYYMMDDxx** (ano com 4 dígitos, mês, dia e quantidade de alterações durante o dia);
7. Refresh ou tempo em que um servidor com a zona replicada tenta replica-la de novo;
8. Intervalo entre tentativas de replicação em caso de falhas;
9. TTL do SOA;
10. Tempo mínino que a zona deve ser retida em memória.

**5.4 – MX e PTR**

Top of Form

Bottom of Form

Os registros **MX** e **PTR** merecem carinho especial dos seus administradores. O formato do registro **MX** é (imaginando o domínio **how2security.com.br**):

***IN MX 10 mail.how2security.com.br***

***IN MX 50 mail2.how2security.com.br***

O **”.”** se refere ao domínio imediatamente superior, ou seja, a zona atual (não se trata de um subdomínio). O número define a preferência do **MX**. Quanto menor o número, maior sua preferência ou prioridade de receber e-mails.

Note que os hostnames **mail.how2security.com.br** e **mail2.how2security.com.br** **DEVEM** ser registros **“A”**, jamais **“CNAME”** nem endereços IP. Embora esses tipos de registros possam funcionar, não estão de acordo com as definições de melhores práticas de DNS publicadas em **RFCs**, e irão causar dores de cabeça ao administrador responsável, uma vez que haverá atrasos e falhas de entrega de e-mails para seu domínio.

Já os registros **PTR** devem estar colocados debaixo de uma zona específica chamada **“in-addr.arpa”**. O registro **PTR** deve ser colocado com os octetos do endereço IP invertidos, e o hostname indicado **PRECISA** existir e apontar para o mesmo endereço IP.

Por exemplo, se tivermos o endereço **200.221.11.98 (UOL)**, seu registro **PTR** seria:

98 IN PTR eliot.uol.com.br

E, obrigatoriamente, para que seu registro **PTR** seja válido e funcional, o host **eliot.uol.com.br** precisa apontar de volta para **200.221.11.98**.

Para consultarmos se nosso reverso está ok, basta rodarmos o seguinte comando:

# dig -x 200.221.11.98

; <<>> DiG 9.5.1-P3 <<>> -x 200.221.11.98

;; global options: printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42805

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:

;98.11.221.200.in-addr.arpa. IN PTR

;; ANSWER SECTION:

98.11.221.200.in-addr.arpa. 3502 IN PTR eliot.uol.com.br.

;; Query time: 1 msec

;; SERVER: 192.168.252.2#53(192.168.252.2)

;; WHEN: Mon Mar 29 22:12:10 2010

;; MSG SIZE rcvd: 74

#

Não é boa ideia ter múltiplos destinos para um mesmo **PTR**, embora isso seja permitido. Tal comportamento pode causar confusão nas aplicações tentando consultar essa informação.

**5.5 – SRV**

Registros **SRV** definem localizações de serviços publicados, inclusive seus protocolos e portas. Um exemplo de registro **SRV** pra **SIP**:

\_sip.\_udp.voip.how2security.com.br. 3600 IN SRV 1 1 5060 voip.how2security.com.br.

O serviço chama-se “**sip**”, **protocolo** **udp**, **3600** segundos de **TTL**, **prioridade 1**, **peso 1** (para registros com mesma prioridade), **porta 5060**, **hostname voip.how2security.com.br**.

Dentro dos **SRVs**, pode-se definir diversos servidores para o mesmo serviço, com prioridades e portas não-convencionais.

Os serviços que usam registros **SRV** mais conhecidos são o protocolo **SIP** de telefonia IP, o protocolo **Jabber** de **Instant Messaging** e, segundo dizem as más línguas, o **Active Directory** daquele outro sistema.

**6 – Protocolo DNS – Referencias**

**Referencias Bibliograficas**

**[1]** Freitas, Andrey Rodrigues de – Perícia forense aplicada à informática: em ambientes Microsoft, 1º Ed, Rio de Janeiro, 2006, Brasport.

**[2]** Forouzan, Behrouz A. – Protocolo TCP/IP, 3º Ed, São Paulo, 2008, McGraw-Hill.

**[3]** Freitas, Andrey Rodrigues de – Perícia forense aplicada à informática: em ambientes Microsoft, 1º Ed, Rio de Janeiro, 2006, Brasport.

**[4]** Registro BR. Disponível em: < http://registro.br/dominio/categoria.html >. Acessado em: 15/04/2014.

**[5]** Gregoriano. Disponível em: <http://www.gregoriano.org.br/portinha/005.htm>. Acessado em: 15/04/2014.

**[6]** Wikipedia. Disponível em: <http://pt.wikipedia.org/wiki/Anexo:Lista\_de\_TLDs>. Acessado em: 16/04/2014.

**[7]** Hugo Azevedo. Disponível em: <http://www.hugoazevedo.eti.br/html/nscd.html>. Acessado em: 05/08/2014.