FUNDAÇÃO UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO
CAMPUS JUAZEIRO
CURSO DE ENGENHARIA DA COMPUTAÇÃO

Breno Gabriel de Souza Coelho

Atividade DNS e prática CMD/Wireshark

Juazeiro, BA
2022

Breno Gabriel de Souza Coelho

Atividade DNS e prática CMD/Wireshark

Relatório requerido pelo professor Fábio Nelson de Sousa Pereira, como parte das exigências de avaliação da disciplina Redes de Computadores I, do curso de Engenharia da Computação, da Universidade do Vale do São Francisco.

Juazeiro, BA
2022

SUMÁRIO

1 INTRODUÇÃO

DNS (Domain Named System) é um protocolo da camada de aplicação responsável, principalmente, pela conversão de nomes de domínio em IP's dos servidores responsáveis pelo nome. Toda vez que um site é acessado (releve a existência de cache DNS por enquanto) o chamado "DNS resolver", software presente no cliente, envia uma mensagem de requisição para um servidor DNS local a fim de obter o IP referente ao nome de domínio.

Isso significa que a navegação web envolve o uso de DNS por natureza, e por isso alguns trabalhos pensam a respeito de como ferramentas de análise do tráfego DNS podem ser utilizadas para identificar possíveis ataques maliciosos via web. ALIEYAN, KAMAL et al (2017), descreve em seu trabalho como o "botnet" é um problema recorrente no qual essa técnica de análise pode se provar útil.

O botnet é um tipo de ataque malicioso via web no qual um computador central (botmaster) infecta uma série de outros dispositivos na rede, que passam a compor a chamada botnet. Ele pode então controlá-los remotamente, realizando ataques DDoS, roubo de dados, interceptação de pacotes, envio de SPAM, sobrecarga de servidores, etc. O trabalho mencionado apresenta vários métodos de detecção de botnets, dando destaque para aqueles baseados em análise DNS. Segundo o autor, esse seria o primeiro artigo de seu conhecimento a apresentar uma revisão direta de métodos de detecção baseados em DNS.

SINGH, MANMEET et al (2019) discutem a respeito dessas técnicas. Ressaltando a forma como os botnets vem se tornando mais sofisticados na última década, assim como mais danosos, e estimando que atualmente existam mais de um milhão de dispositivos infectados. O artigo destaca que há poucas produções voltadas para desenvolver um método de detecção de botnets através do DNS, e critica os já existentes por "não compreenderem ou não levarem em consideração diversos parâmetros essenciais para uma comparação efetiva"

No início dos anos 2000, com o boom da internet, alguns artigos discutiam sobre as tecnologias à época e suas formas de fornecer aos usuários um serviço compatível com a crescente importância e demanda desses meios. Fazendo uma análise de caso com a empresa provedora de conteúdos Akamai, eles analisam os esquemas de seleção de servidor DNS da empresa, e outros detalhes. Além disso, fazem uma análise geral de outros pontos relativos a atuação web da empresa, ao final apresentando insights sobre mudanças que poderiam ser realizadas em outros servidores a fim de suportar melhorias (PAN, JIANPING et al, 2003).

Como visto, desde o início do século, alguns autores, mesmo reconhecendo a importância do DNS, entendem que o avanço da internet e o aumento do número de usuários/páginas esclarece alguns problemas nos protocolos já existentes. Para SHAIKH, ANEES et al (2010), a tendência à época de reduzir os valores TTL ou até mesmo eliminá-los era capaz de estender os tempos de acesso à informação de maneira preocupante; segundo seu trabalho, em até duas ordens de magnitude.Outro problema mencionado foi, em suas palavras, "o entendimento

implícito que nameservers clientes são um indicador são indicativos da localização real ou performance desses". Usando os logs de servidor de mensagens HTTP e DNS, junto de um grande número de ISP discadas, mostraram que uma fração significativa dos nameservers clientes na verdade se encontravam a uma distância considerável, com mais de 8 pulos sendo necessários para alcançá-los.

No entanto, alguns desses argumentos eram contestados. JUNG, JAEYEON et al (2002) apresenta em seu texto um conjunto de testes sobre a eficiência do caching DNS através da análise dos traços DNS e tráfego TCP coletado através de conexões do servidor do MIT e o KAIST (Korea Advanced Institute of Science and Technology). Não vou detalhar os resultados obtidos, mas eles apresentaram uma porcentagem significativa de erros/problemas nos envios de pacotes (os lookups tiveram uma taxa de cerca de 20% de ausência de resposta, porém mais da metade de todos os pacotes DNS traçados foram contabilizados nesse percentual, devido ao grande número de retransmissões de pacote), além disso, o que possivelmente é o ponto mais importante é a percepção de que baixos valores de TTL (tão baixos quanto algumas centenas de segundos) teve pouco efeito nas taxas de sucesso (hit rates), e pouco benefício foi alcançado com o compartilhamento adiantado de cache DNS em cerca de 10 à 20 clientes.

Esse artigo, quando comparado com o passado (que mencionava um aumento nos tempos de acesso à informação em pacotes de baixo TTL) parecem dialogar, no início dos anos 2000, sobre alguns parâmetros e medidas mais apropriados para o funcionamento do DNS, em especial aos valores TTL dos cache DNS. Aparentemente houve algum debate sobre o assunto na época, provavelmente estimulado pelo aumento no uso e demanda da web (com o surgimento da chamada web 2.0) em tais anos.

2 METODOLOGIA

Perguntas feitas no arquivo:

1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in

2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?

5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number6 in the trace for the DNS query message? Is this query message sent over UDP or TCP?

6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

7. What is the destination port for the DNS query message? What is the source port of the DNS response message?

8. To what IP address is the DNS query message sent?

9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

10. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file

http://gaia.cs.umass.edu/kurose_ross/? What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address? What is the packet number in the trace of the received DNS response? What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg? What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address? Discuss how DNS caching affects the answer to this last question.

12. What is the destination port for the DNS query message? What is the source port of the DNS response message?

13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

14. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

17. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?

18. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records?

3 DISCUSSÃO

```
C:\Users\Anduin110>nslookup www.iitb.ac.in.
Servidor:  ip-177.71.92.18.juniornet.psi.br
Address:  177.71.92.18

Não é resposta autoritativa:
Nome:    www.iitb.ac.in
Address:  103.21.124.10
```

1. Usando a aplicação “nslookup”, obtemos o vlaor de IP : 103.21.124.10
2. A resposta foi fornecida pelo nameserver de IP 177.71.92.18 (pelo nome dele, pertencente a Jr Net - minha ISP)
3. Veio de um nameserver não autoritativo. Possivelmente meu nameserver local realizou uma busca iterativa e/ou recursiva e acabou encontrando um RR correspondente no cache de algum outro nameserver.

```
C:\Users\Anduin110>nslookup -type=NS iitb.ac.in.
Servidor:  ip-177.71.92.18.juniornet.psi.br
Address:  177.71.92.18

Não é resposta autoritativa:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in
```

4. O primeiro servidor autoritativo para esse domínio que foi obtido é o dns1.iitb.ac.in. Utilizando o comando “nslookup” para esse domínio. Inclusive fazendo isso o IP obtido é 103.21.125.129.

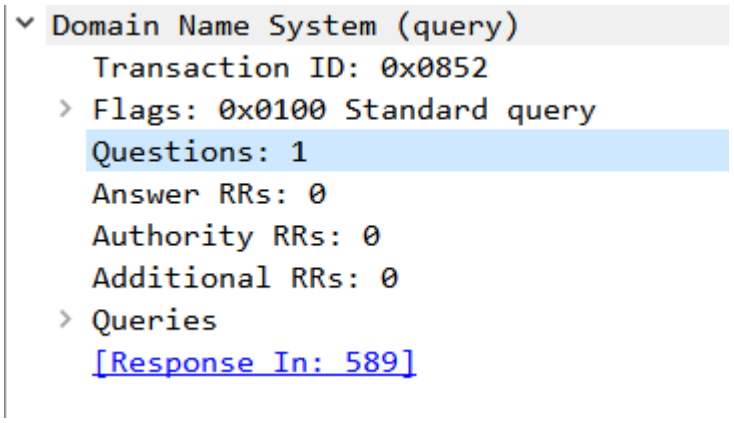
```
> Frame 588: 77 bytes on wire (616 bits), 77 bytes captured (616
> Ethernet II, Src: Palladiu_da:b3:3f (5c:c9:d3:da:b3:3f), Dst:
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 177.71.9
> User Datagram Protocol, Src Port: 63294, Dst Port: 53
> Domain Name System (query)
```

(DNS query)

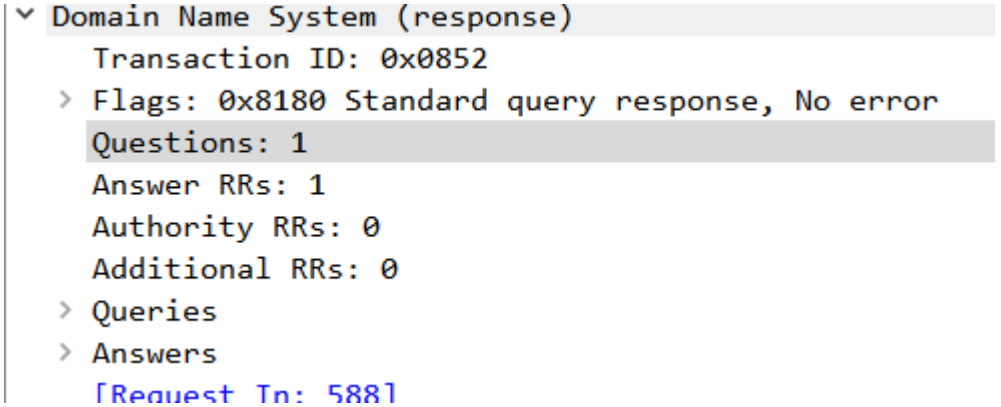
```
> Frame 589: 93 bytes on wire (744 bits), 93 bytes captured (744 bi
> Ethernet II, Src: TendaTec_86:e6:00 (cc:2d:21:86:e6:00), Dst: Pal
> Internet Protocol Version 4, Src: 177.71.92.18, Dst: 192.168.0.10
> User Datagram Protocol, Src Port: 53, Dst Port: 63294
> Domain Name System (response)
```

(DNS response)

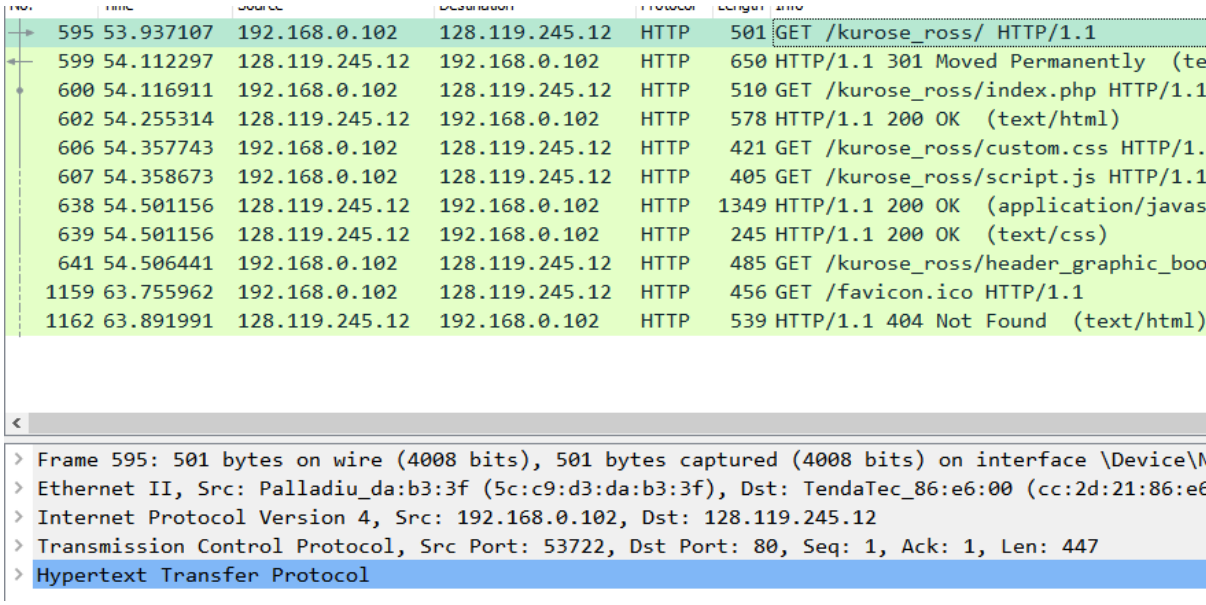
5. Na minha captura, foi o pacote de número 588. Olhando os detalhes do pacote DNS, posso ver que ele possui associado um User Datagram Protocol, logo foi enviado usando o protocolo UDP.
6. O pacote de resposta foi recebido logo em seguida, é o 589. Ele também foi transportado com o protocolo UDP.
7. Diretamente pelo detalhamento, podemos ver que o pacote pergunta foi enviado para a porta 53. Abrindo o detalhamento UDP do segundo pacote (de resposta) vemos que ele foi enviado da porta 53 também. A porta para qual o pacote foi inicialmente enviado é igual àquela na qual foi recebido.
8. O pacote de pergunta foi enviado para o IP 177.71.92.18 (da pra ver um pedacinho na foto ali encima, ou você pode ver inteiro no “source” da resposta)



9. Uma pergunta, nenhuma resposta.



10. Uma pergunta (que é uma cópia daquela que foi feita) e uma resposta.

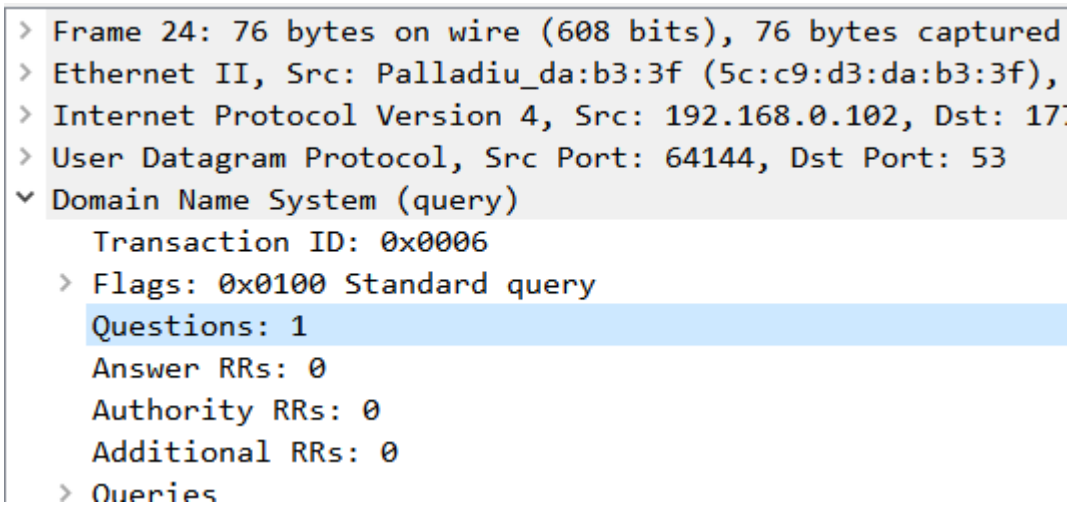


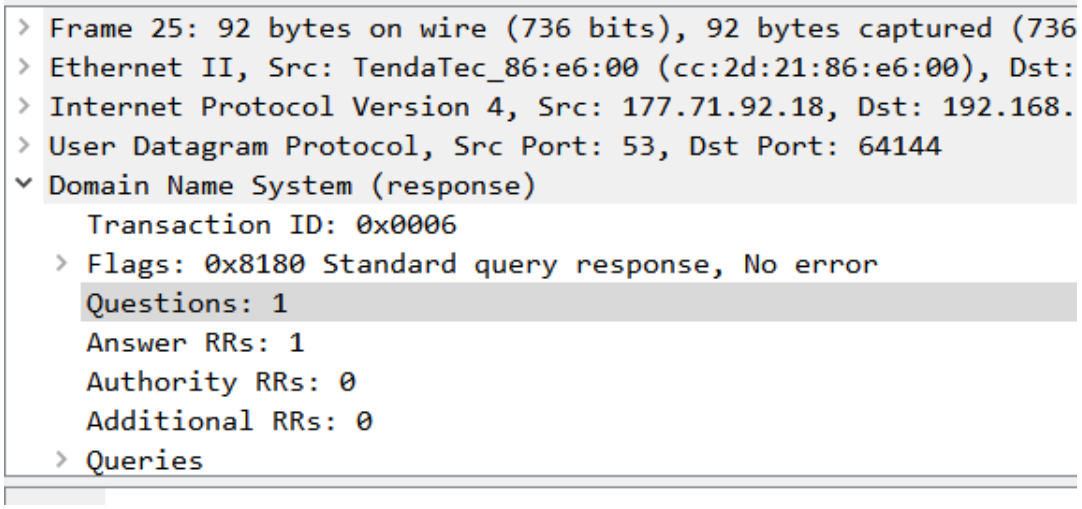
No.	Time	Source	Destination	Protocol	Length	Info
595	53.937107	192.168.0.102	128.119.245.12	HTTP	501	GET /kurose_ross/ HTTP/1.1
599	54.112297	128.119.245.12	192.168.0.102	HTTP	650	HTTP/1.1 301 Moved Permanently (te
600	54.116911	192.168.0.102	128.119.245.12	HTTP	510	GET /kurose_ross/index.php HTTP/1.1
602	54.255314	128.119.245.12	192.168.0.102	HTTP	578	HTTP/1.1 200 OK (text/html)
606	54.357743	192.168.0.102	128.119.245.12	HTTP	421	GET /kurose_ross/custom.css HTTP/1.
607	54.358673	192.168.0.102	128.119.245.12	HTTP	405	GET /kurose_ross/script.js HTTP/1.1
638	54.501156	128.119.245.12	192.168.0.102	HTTP	1349	HTTP/1.1 200 OK (application/javas
639	54.501156	128.119.245.12	192.168.0.102	HTTP	245	HTTP/1.1 200 OK (text/css)
641	54.506441	192.168.0.102	128.119.245.12	HTTP	485	GET /kurose_ross/header_graphic_boo
1159	63.755962	192.168.0.102	128.119.245.12	HTTP	456	GET /favicon.ico HTTP/1.1
1162	63.891991	128.119.245.12	192.168.0.102	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```
> Frame 595: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\N
> Ethernet II, Src: Palladiu_da:b3:3f (5c:c9:d3:da:b3:3f), Dst: TendaTec_86:e6:00 (cc:2d:21:86:e6
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53722, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
> Hypertext Transfer Protocol
```

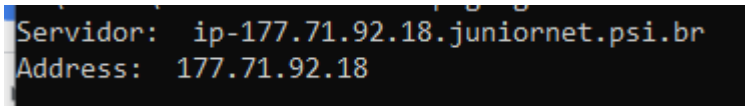
11. Pacote número 595. Esse é o pacote HTTP com a mensagem de requisição para a página html.
    O pacote DNS apresentado anteriormente foi enviado a fim de resolver o endereço DNS do nome de domínio. Como mencionado, seu número era 588. A resposta então veio no 589.
    Olhando na imagem acima, vemos que foi o pacote 641. Analisando o trace das requisições DNS, não encontrei nenhuma outra busca de resolução para o nome “gaia.cs.umass.edu”. Certamente o RR obtido foi guardado no meu cache DNS e por isso não foi feita outra busca..
    Usando o comando “ipconfig /displaydns” podemos ver que realmente a resolução DNS está em cache:

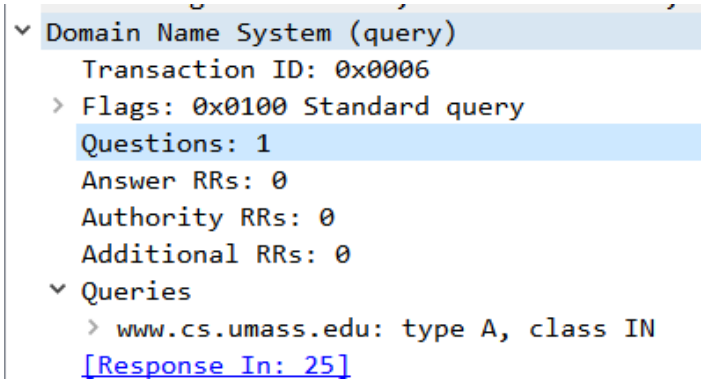
```
gaia.cs.umass.edu
----------------------------------------
 Nome do Registro. . . . . . . . . . . . : gaia.cs.umass.edu
 Tipo de Registro. . . . . . . . . . . . : 1
 Tempo de Vida . . . . . . . . . . . . . : 19969
 Comprimento dos Dados . . . . . . . . . : 4
Seção. . . . . . . . . . . . . . . . . . : Resposta
Registro (Host). . . . . . . . . . . . . : 128.119.245.12
```



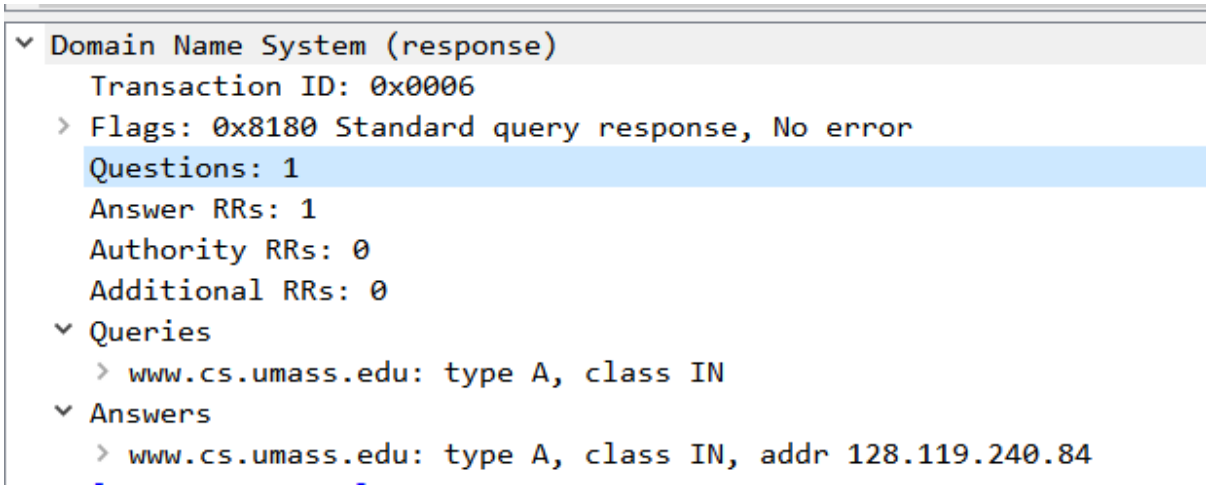


12. Pelas imagens acima, que representam o pedido e a resposta (respectivamente), a porta de destino para o pedido foi 53. A porta fonte na resposta foi a mesma, 53, como esperado.
13. Foi enviada para o IP 177.71.92.18. Usando o “nslookup” verifiquei que de fato esse é o IP do meu servidor DNS local:

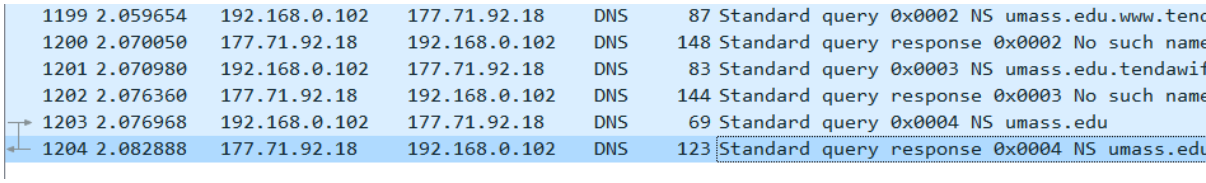




14. Examinando a imagem acima, vemos que há somente 1 pedido, sem nenhuma resposta, e ele é do tipo A. (resolução IP)



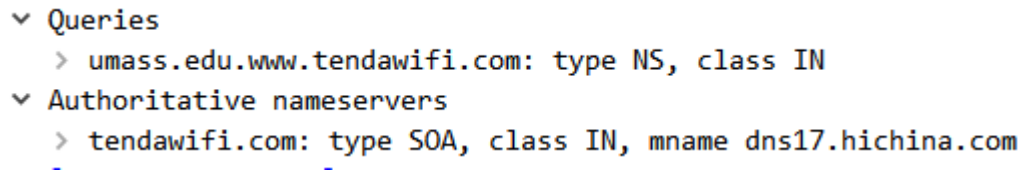
15. Possui uma pergunta, que é a enviada no “query”, e uma resposta, na forma de um RR que inclusive pode ser visto na imagem acima.

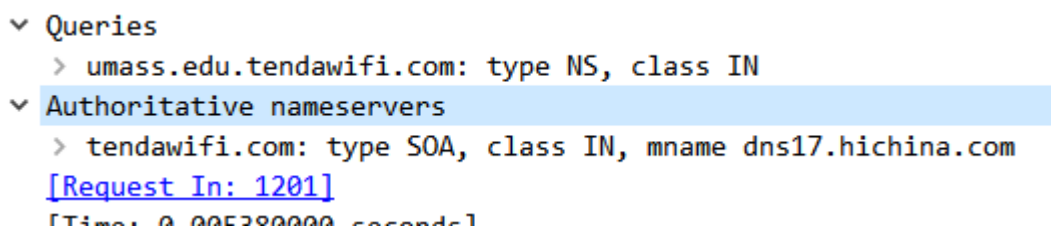


16. Algumas mensagens DNS foram enviadas. Somente a última conseguiu o resultado correto, as primeiras não encontraram os nomes procurados nos nameservers acessados. Contudo, esses informaram o endereço de outros nameservers autoritativos para que a busca fosse continuada (procedimento iterativo). Analisando a imagem, pode-se ver que todos os pacotes foram enviados para o IP do meu servidor DNS local, 177.71.92.18.

17. Em todos os envios de “query” somente uma pergunta foi enviada, que era o nameserver autoritativo para o domínio dado. Nenhuma resposta estava presente nos pacotes de pedido.

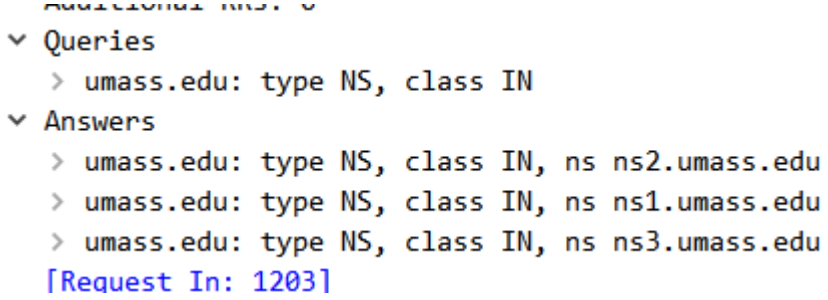
18. As primeiras duas respostas possuíam as seguintes respostas:



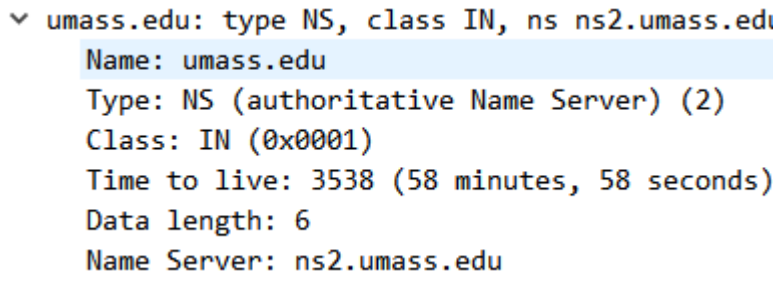


Tecnicamente não são respostas, mas sim “Authoritative nameservers” Olhando com maior atenção vemos que o nome do nameserver retornado nas mensagens é o mesmo (dns17.hichina.com), o que mudou foi a pergunta. Inicialmente, foi buscado o nome “umass.edu.www.tendawifi.com”, depois foi buscado “umass.edu.tendawifi.com”. Ambas as “respostas” são da forma de um registro SOA, com vários dados que ao que eu verifiquei estavam iguais.

O terceiro pedido, no entanto, endereçado para “umass.edu”, teve resultado:



Foram enviadas três respostas, contendo os nameservers responsáveis pela zona “umass.edu”. Cada uma dessas respostas possuía uma série de dados adicionais, seis ao total:



Aqui temos o nome da zona buscada (umass.edu), o tipo da busca (NS), a classe (IN - Internet), o TTL (tempo para que o RR seja apagado de um cache, inclusive do meu computador), o comprimento do arquivo – 6 – (quantidade de dados adicionais ?) e o que foi buscado, o nome do nameserver. (cada uma das três respostas trouxe um)

4 CONCLUSÃO

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

5 REFERÊNCIA BIBLIOGRÁFICA

ALIEYAN, KAMALI et al. **A survey of botnet detection based on DNS.** Neural Computing and Applications, v. 28, n. 7, p. 1541-1558 (2017).

SINGH, MANMEET; SINGH, MANINDER; KAUR, SANMEET. **Issues and challenges in DNS based botnet detection: A survey.** Computers & Security, v. 86, p. 28-52 (2019.

PAN, JIANPING; HOU, Y. THOMAS; LI, BO. **An overview of DNS-based server selections in content distribution networks.** Computer Networks, v. 43, n. 6, p. 695-711 (2003)

SHAIKH, ANEES; TEWARI, RENU; AGRAWAL, MUKESH. **On the effectiveness of DNS-based server selection.** In: Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213). IEEE p. 1801-1810. (2001)

JUNG, JAEYEON et al. **DNS performance and the effectiveness of caching. IEEE/ACM Transactions on networking,** v. 10, n. 5, p. 589-603 (2002)