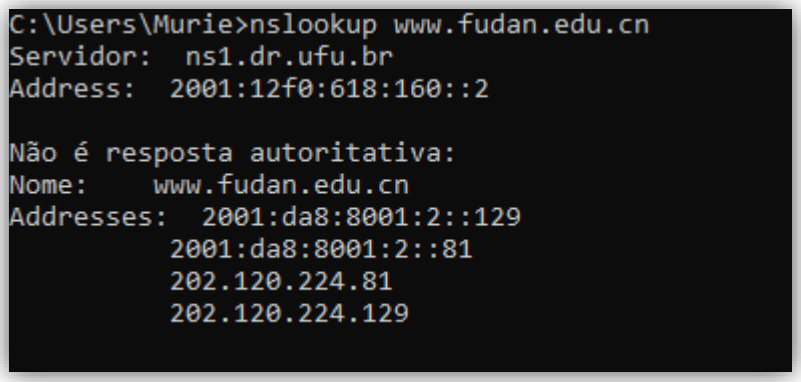
GSI023 – Redes de Computadores

Wireshark Lab - DNS

Murielly Oliveira Nascimento – 11921BSI222 – murielly.nascimento@ufu.br

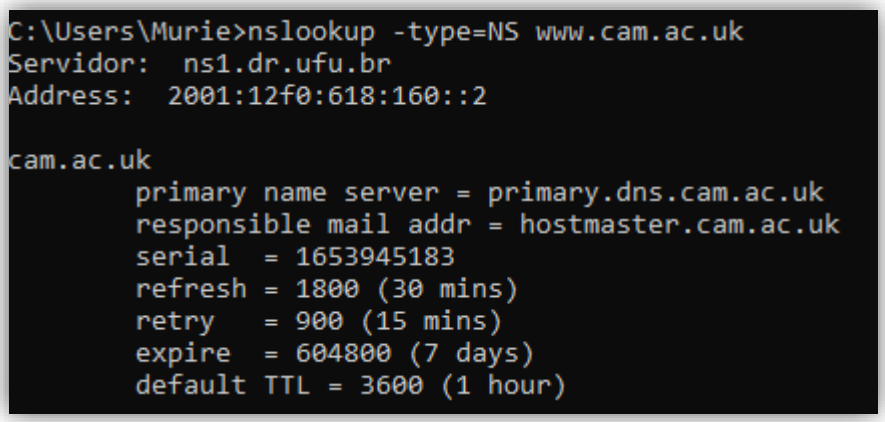
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

O endereço IP é 2001:da8:8001:2::129



2. Run nslookup to determine the authoritative DNS servers for a university in Europe

O DNS autoritativo é primary.dns.cam.ac.uk



3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

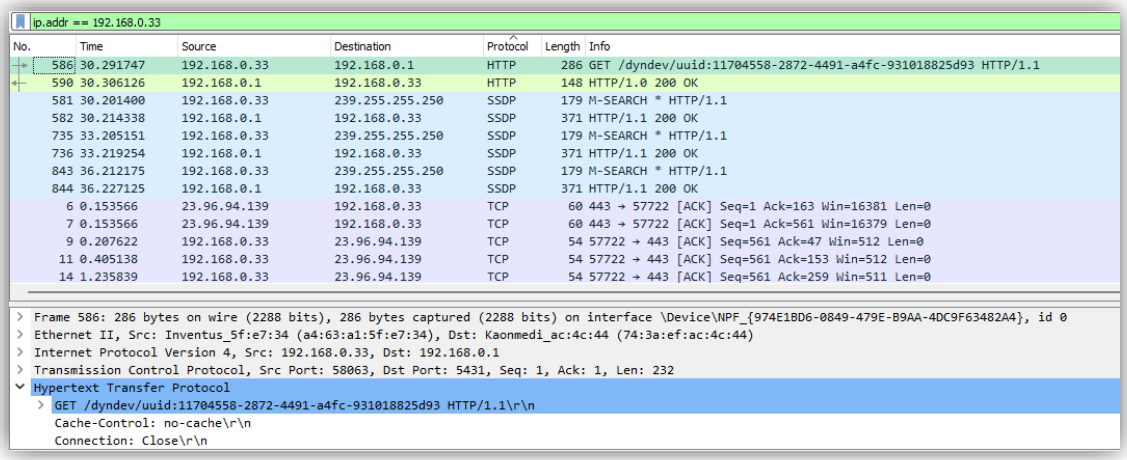
O endereço IP é 2804:1bc:f038:1fa:3000

```
C:\Users\Murie>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  2804:1bc:f038:1fa::3000

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** O tempo limite da solicitação para UnKnown expirou
```

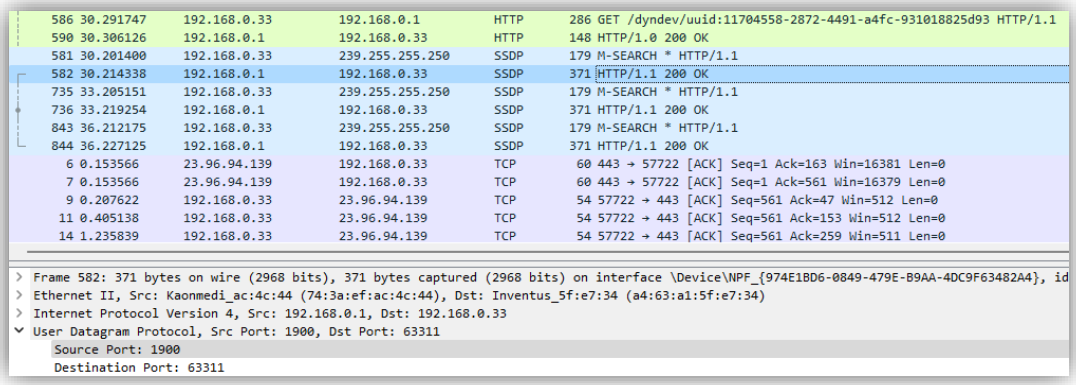
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

São enviadas pelo UDP



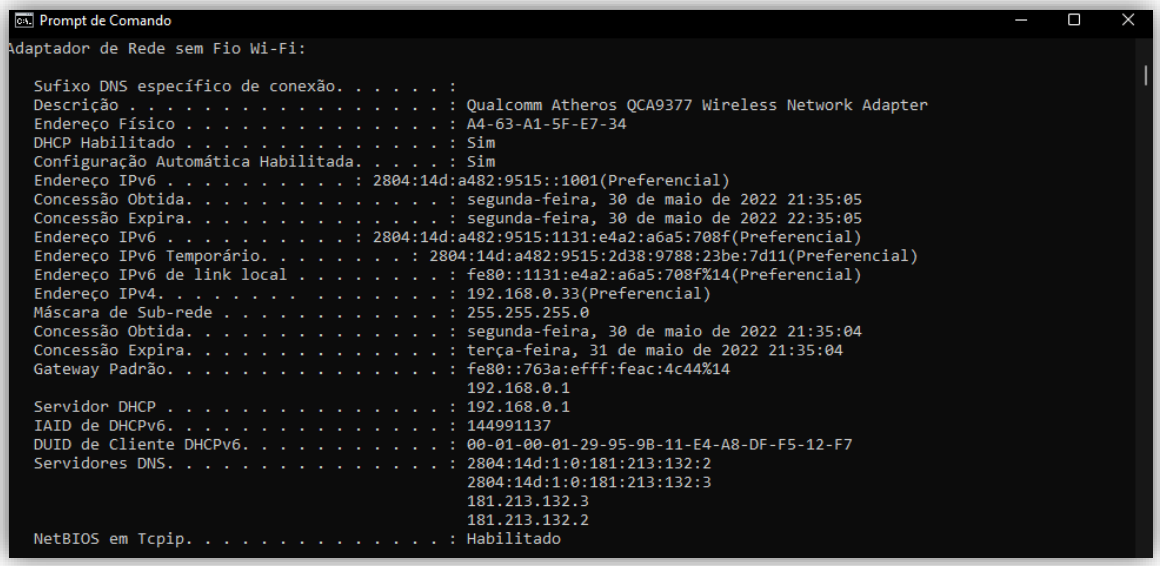
5. What is the destination port for the DNS query message? What is the source port of DNS response message?

O destination port é 1900 e o source pot é 63311.



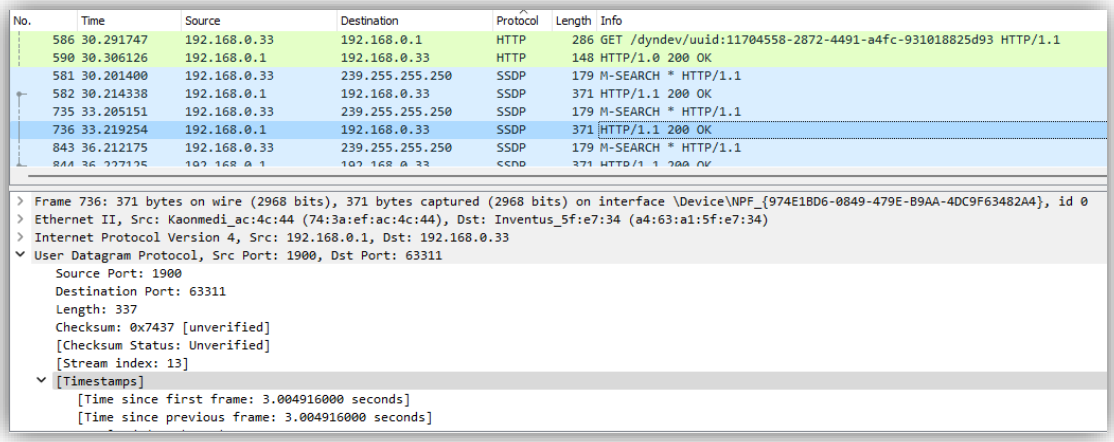
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

O meu endereço IP local é 192.168.0.33 que é um dos endereços IP de um dos servidores DNS locais.



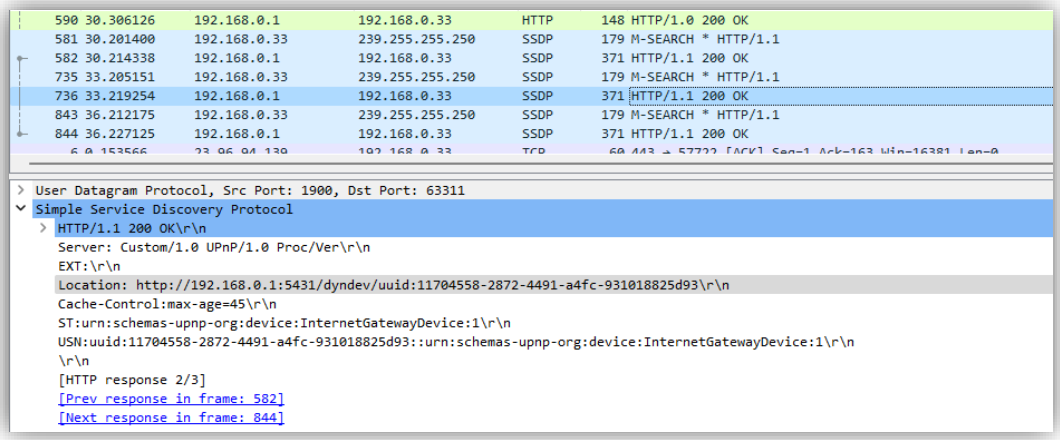
7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

É um tipo regular de DNS quey e não exibe nenhuma resposta.



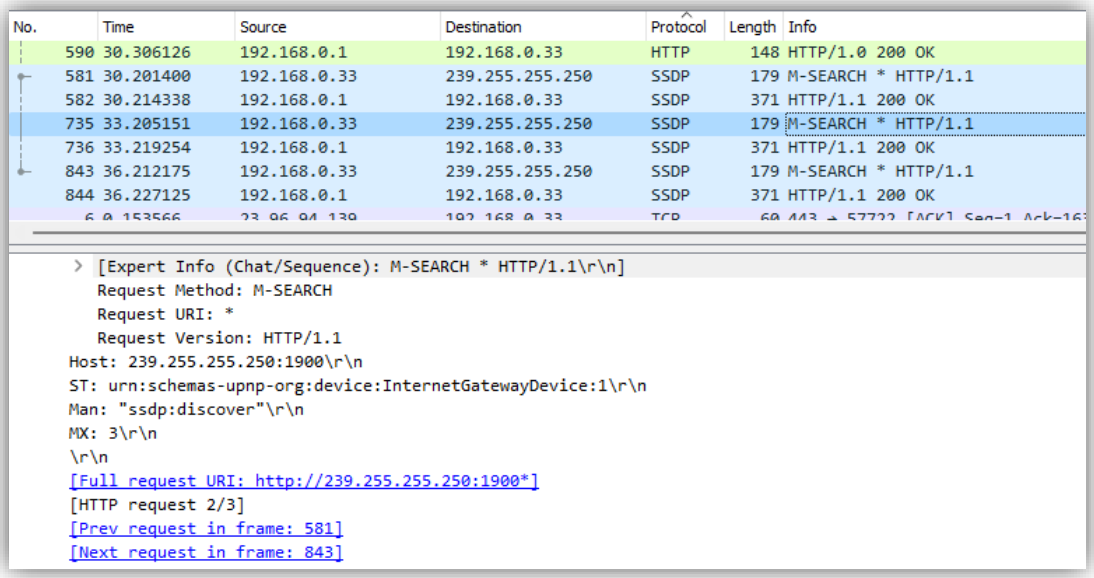
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

São 3 respostas contendo o endereço do site.



9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

O primeiro pacote SYN foi enviado para o IP 239.255.255.250 que é o mesmo IP fornecido na mensagem de resposta DNS.

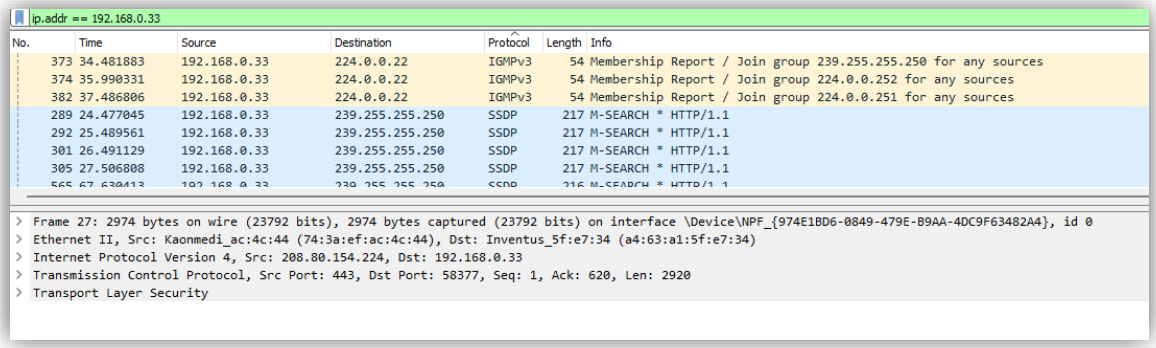


10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Não.

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

O destination port é 1900 e o source pot é 63311.



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

É o endereço IP padrão do servidor DNS 192.168.0.33, obtido quando usamos o comando ipconfig –all.

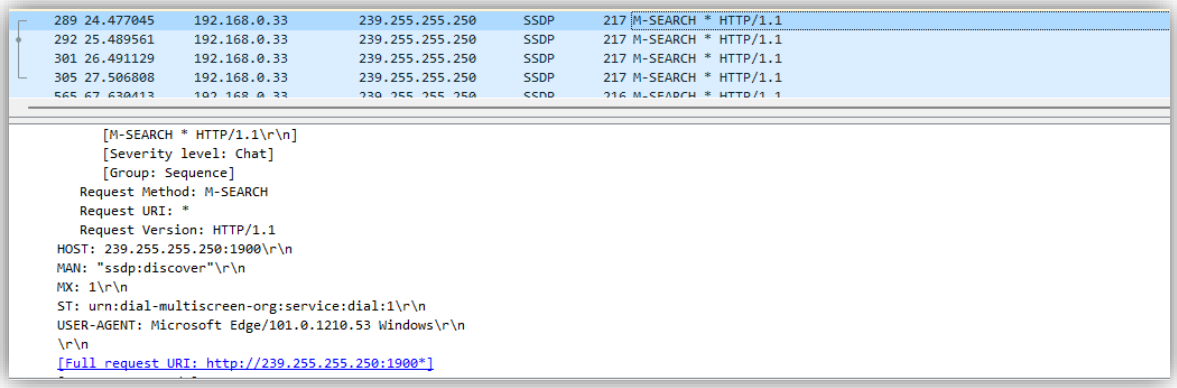
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

É do tipo A e não contém respostas.

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

A resposta DNS contém o nome do host, o endereço IP e a classe.

15. Provide a screenshot.



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

É enviado para o endereço IP 192.168.0.33 que é o meu endereço IP para o servidor DNS local.

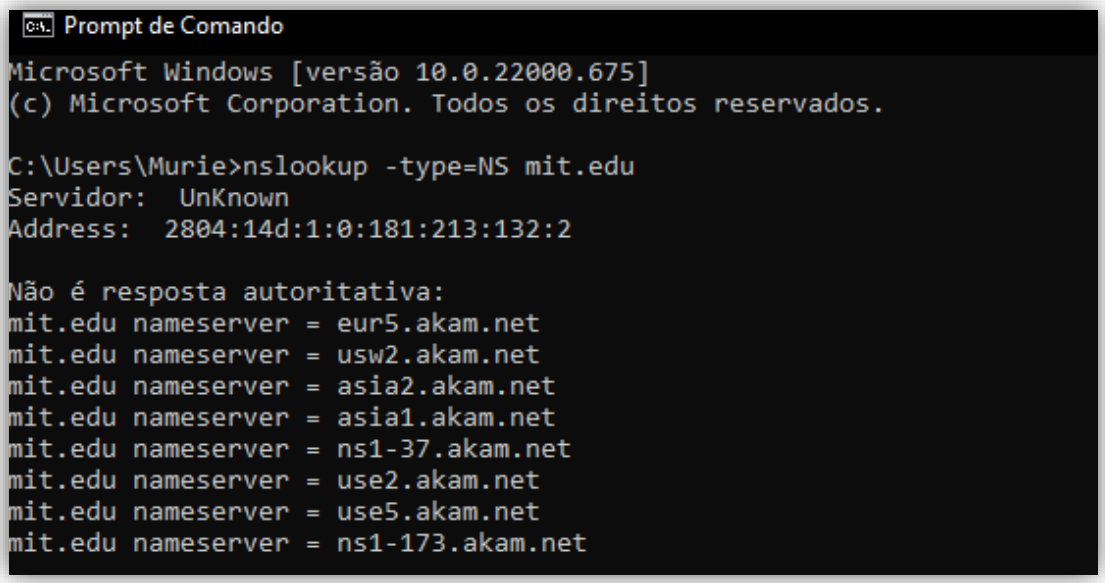
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

É do tipo NS DNS e não contém respostas.

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

São mostrados os servidores, mas não os seus endereços. Os nameservers são eur5.akam.net, usw2.akam.net, asia2.akam.nete ns1-173.akam.nt.

19. Provide a screenshot.



20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

A query foi enviada para o endereço IP 18.0.72.3 que é o endereço do site do MIT.

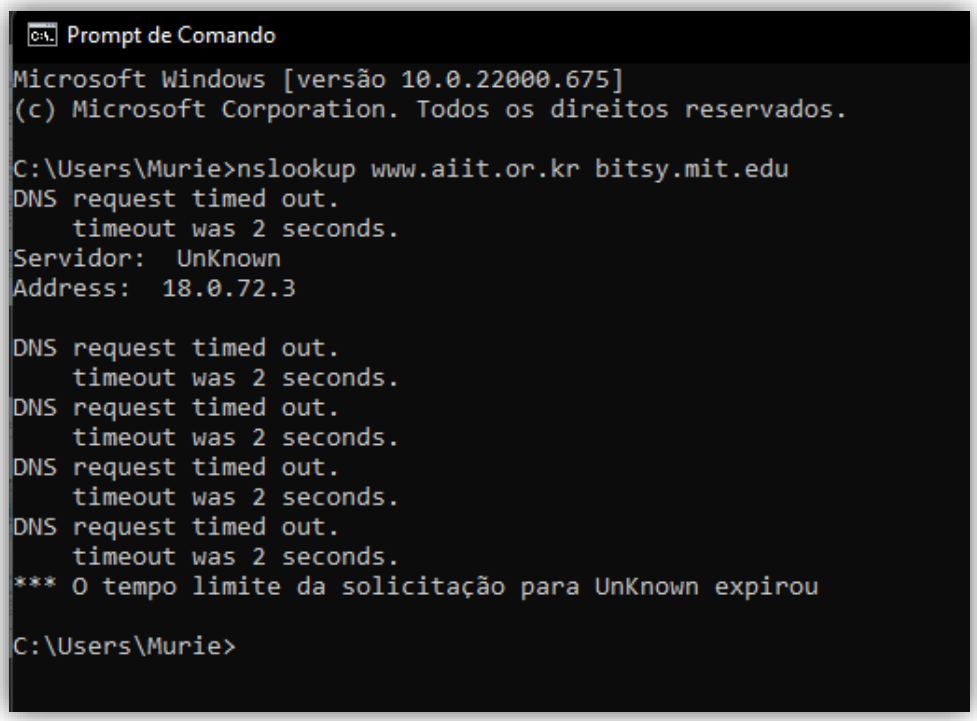
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

É do tipo regular A e não contém respostas

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?

É providenciada uma resposta contendo o endereço e informações do site.

23. Provide a screenshot


Prompt de Comando
Microsoft Windows [versão 10.0.22000.675]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\Murie>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
timeout was 2 seconds.
Servidor: UnKnown
Address: 18.0.72.3
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** O tempo limite da solicitação para UnKnown expirou
C:\Users\Murie>