

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

```
C:\Users\Murie>nslookup www.fudan.edu.cn
Servidor: ns1.dr.ufu.br
Address: 2001:12f0:618:160::2

Não é resposta autoritativa:
Nome: www.fudan.edu.cn
Addresses: 2001:da8:8001:2::129
           2001:da8:8001:2::81
           202.120.224.81
           202.120.224.129
```

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

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

```
C:\Users\Murie>nslookup -type=NS www.cam.ac.uk
Servidor: ns1.dr.ufu.br
Address: 2001:12f0:618:160::2

cam.ac.uk
primary name server = primary.dns.cam.ac.uk
responsible mail addr = hostmaster.cam.ac.uk
serial = 1653945183
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

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

No.	Time	Source	Destination	Protocol	Length	Info
586	30.291747	192.168.0.33	192.168.0.1	HTTP	286	GET /dyndev/uuid:11704558-2872-4491-a4fc-931018825d93 HTTP/1.1
590	30.306126	192.168.0.1	192.168.0.33	HTTP	148	HTTP/1.0 200 OK
581	30.201400	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
582	30.214338	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
735	33.205151	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
736	33.219254	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
843	36.212175	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
844	36.227125	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
6	0.153566	23.96.94.139	192.168.0.33	TCP	60	443 → 57722 [ACK] Seq=1 Ack=163 Win=16381 Len=0
7	0.153566	23.96.94.139	192.168.0.33	TCP	60	443 → 57722 [ACK] Seq=1 Ack=561 Win=16379 Len=0
9	0.207622	192.168.0.33	23.96.94.139	TCP	54	57722 → 443 [ACK] Seq=561 Ack=47 Win=512 Len=0
11	0.405138	192.168.0.33	23.96.94.139	TCP	54	57722 → 443 [ACK] Seq=561 Ack=153 Win=512 Len=0
14	1.235839	192.168.0.33	23.96.94.139	TCP	54	57722 → 443 [ACK] Seq=561 Ack=259 Win=511 Len=0

> Frame 586: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
> Ethernet II, Src: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34), Dst: Kaonmedi_ac:4c:44 (74:3a:ef:ac:4c:44)
> Internet Protocol Version 4, Src: 192.168.0.33, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 58063, Dst Port: 5431, Seq: 1, Ack: 1, Len: 232
> Hypertext Transfer Protocol
> GET /dyndev/uuid:11704558-2872-4491-a4fc-931018825d93 HTTP/1.1\r\n
Cache-Control: no-cache\r\n
Connection: Close\r\n

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.

586	30.291747	192.168.0.33	192.168.0.1	HTTP	286	GET /dyndev/uuid:11704558-2872-4491-a4fc-931018825d93 HTTP/1.1
590	30.306126	192.168.0.1	192.168.0.33	HTTP	148	HTTP/1.0 200 OK
581	30.201400	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
582	30.214338	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
735	33.205151	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
736	33.219254	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
843	36.212175	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
844	36.227125	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
6	0.153566	23.96.94.139	192.168.0.33	TCP	60	443 → 57722 [ACK] Seq=1 Ack=163 Win=16381 Len=0
7	0.153566	23.96.94.139	192.168.0.33	TCP	60	443 → 57722 [ACK] Seq=1 Ack=561 Win=16379 Len=0
9	0.207622	192.168.0.33	23.96.94.139	TCP	54	57722 → 443 [ACK] Seq=561 Ack=47 Win=512 Len=0
11	0.405138	192.168.0.33	23.96.94.139	TCP	54	57722 → 443 [ACK] Seq=561 Ack=153 Win=512 Len=0
14	1.235839	192.168.0.33	23.96.94.139	TCP	54	57722 → 443 [ACK] Seq=561 Ack=259 Win=511 Len=0

> Frame 582: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id
> Ethernet II, Src: Kaonmedi_ac:4c:44 (74:3a:ef:ac:4c:44), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.33
✓ User Datagram Protocol, Src Port: 1900, Dst Port: 63311
Source Port: 1900
Destination Port: 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.

```

Prompt de Comando
Adaptador de Rede sem Fio Wi-Fi:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Endereço Físico . . . . . : A4-63-A1-5F-E7-34
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . : Sim
Endereço IPv6 . . . . . : 2804:14d:a482:9515::1001(Preferencial)
Concessão Obtida. . . . . : segunda-feira, 30 de maio de 2022 21:35:05
Concessão Expira. . . . . : segunda-feira, 30 de maio de 2022 22:35:05
Endereço IPv6 . . . . . : 2804:14d:a482:9515:1131:e4a2:a6a5:708f(Preferencial)
Endereço IPv6 Temporário. . . . . : 2804:14d:a482:9515:2d38:9788:23be:7d11(Preferencial)
Endereço IPv6 de link local . . . . . : fe80::1131:e4a2:a6a5:708f%14(Preferencial)
Endereço IPv4. . . . . : 192.168.0.33(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : segunda-feira, 30 de maio de 2022 21:35:04
Concessão Expira. . . . . : terça-feira, 31 de maio de 2022 21:35:04
Gateway Padrão. . . . . : fe80::763a:efff:feac:4c44%14
                          192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID de DHCPv6. . . . . : 144991137
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-29-95-9B-11-E4-A8-DF-F5-12-F7
Servidores DNS. . . . . : 2804:14d:1:0:181:213:132:2
                          2804:14d:1:0:181:213:132:3
                          181.213.132.3
                          181.213.132.2
NetBIOS em Tcpip. . . . . : Habilitado

```

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 query e não exibe nenhuma resposta.

No.	Time	Source	Destination	Protocol	Length	Info
586	30.291747	192.168.0.33	192.168.0.1	HTTP	286	GET /dyndev/uuid:11704558-2872-4491-a4fc-931018825d93 HTTP/1.1
590	30.306126	192.168.0.1	192.168.0.33	HTTP	148	HTTP/1.0 200 OK
581	30.201400	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
582	30.214338	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
735	33.205151	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
736	33.219254	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
843	36.212175	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
844	36.227125	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK

> Frame 736: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0
 > Ethernet II, Src: Kaonmedi_ac:4c:44 (74:3a:ef:ac:4c:44), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.33
 > User Datagram Protocol, Src Port: 1900, Dst Port: 63311
 Source Port: 1900
 Destination Port: 63311
 Length: 337
 Checksum: 0x7437 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 13]
 [Timestamps]
 [Time since first frame: 3.004916000 seconds]
 [Time since previous frame: 3.004916000 seconds]

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.

590	30.306126	192.168.0.1	192.168.0.33	HTTP	148	HTTP/1.0 200 OK
581	30.201400	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
582	30.214338	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
735	33.205151	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
736	33.219254	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
843	36.212175	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
844	36.227125	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK

> User Datagram Protocol, Src Port: 1900, Dst Port: 63311
 > Simple Service Discovery Protocol
 > HTTP/1.1 200 OK\r\n
 Server: Custom/1.0 UPnP/1.0 Proc/Ver\r\n
 EXT:\r\n
 Location: http://192.168.0.1:5431/dyndev/uuid:11704558-2872-4491-a4fc-931018825d93\r\n
 Cache-Control:max-age=45\r\n
 ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
 USN:uuid:11704558-2872-4491-a4fc-931018825d93:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
 \r\n
 [HTTP response 2/3]
 [\[Prev response in frame: 582\]](#)
 [\[Next response in frame: 844\]](#)

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.

No.	Time	Source	Destination	Protocol	Length	Info
590	30.306126	192.168.0.1	192.168.0.33	HTTP	148	HTTP/1.0 200 OK
581	30.201400	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
582	30.214338	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
735	33.205151	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
736	33.219254	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
843	36.212175	192.168.0.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
844	36.227125	192.168.0.1	192.168.0.33	SSDP	371	HTTP/1.1 200 OK
60	153566	239.255.255.250	192.168.0.33	TCP	60	443 → 57777 [ACK] Seq=1 Ack=16

> [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]

Request Method: M-SEARCH

Request URI: *

Request Version: HTTP/1.1

Host: 239.255.255.250:1900\r\n

ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n

Man: "ssdp:discover"\r\n

MX: 3\r\n

\r\n

[\[Full request URI: http://239.255.255.250:1900*\]](#)

[\[HTTP request 2/3\]](#)

[\[Prev request in frame: 581\]](#)

[\[Next request in frame: 843\]](#)

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 port é 63311.

No.	Time	Source	Destination	Protocol	Length	Info
373	34.481883	192.168.0.33	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
374	35.990331	192.168.0.33	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
382	37.486806	192.168.0.33	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
289	24.477045	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
292	25.489561	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
301	26.491129	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
305	27.506808	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
565	67.630412	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

> Frame 27: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface \Device\NPF_{974E1BD6-0849-479E-B9AA-4DC9F63482A4}, id 0

> Ethernet II, Src: Kaonmedi_ac:4c:44 (74:3a:ef:ac:4c:44), Dst: Inventus_5f:e7:34 (a4:63:a1:5f:e7:34)

> Internet Protocol Version 4, Src: 208.80.154.224, Dst: 192.168.0.33

> Transmission Control Protocol, Src Port: 443, Dst Port: 58377, Seq: 1, Ack: 620, Len: 2920

> Transport Layer Security

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.

No.	Time	Source	Destination	Protocol	Length	Info
289	24.477045	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
292	25.489561	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
301	26.491129	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
305	27.506808	192.168.0.33	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Details of packet 292
[M-SEARCH * HTTP/1.1\r\n
[Severity level: Chat]
[Group: Sequence]
Request Method: M-SEARCH
Request URI: *
Request Version: HTTP/1.1
HOST: 239.255.255.250:1900\r\n
MAN: "ssdp:discover"\r\n
MX: 1\r\n
ST: urn:dial-multiscreen-org:service:dial:1\r\n
USER-AGENT: Microsoft Edge/101.0.1210.53 Windows\r\n
\r\n
[Full request URI: http://239.255.255.250:1900*]

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.

```

C:\> Prompt de Comando

Microsoft Windows [versão 10.0.22000.675]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\Murie>nslookup -type=NS mit.edu
Servidor: UnKnown
Address: 2804:14d:1:0:181:213:132:2

Não é resposta autoritativa:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-173.akam.net

```

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

C:\ 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>