

Aluno: Gustavo de Souza Braga  
Turma: 2b

## Etapa 2

1. Com Wireshark ativo (Abra-o novamente) faça um ping para um site conhecido (você pode usar o nome: www.google.br por exemplo):

The screenshot shows a Windows command prompt window with the following commands and output:

```
C:\Users\gustavo_s_braga>C:\> nslookup myip.opendns.com. resolver1.opendns.com
'C:\' não é reconhecido como um comando interno
ou externo, um programa operável ou um arquivo em lotes.

C:\Users\gustavo_s_braga> nslookup myip.opendns.com. resolver1.opendns.com
Servidor: dns.opendns.com
Address: 208.67.222.222

Não é resposta autoritativa:
Nome: myip.opendns.com
Address: 189.8.205.19

C:\Users\gustavo_s_braga>ping www.google.com

Disparando www.google.com [142.251.129.132] com 32 bytes de dados:
Resposta de 142.251.129.132: bytes=32 tempo=12ms TTL=118
Resposta de 142.251.129.132: bytes=32 tempo=13ms TTL=118
Resposta de 142.251.129.132: bytes=32 tempo=12ms TTL=118
Resposta de 142.251.129.132: bytes=32 tempo=12ms TTL=118

Estatísticas do Ping para 142.251.129.132:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 12ms, Máximo = 13ms, Média = 12ms

C:\Users\gustavo_s_braga>
```

Overlaid on top of the command prompt is a Wireshark packet capture window showing ICMPv6 traffic. The packet list shows several echo requests and replies between 10.3.119.43 and 142.251.129.132.

No.	Time	Source	Destination	Protocol	Length	Info
9829	216.421656	10.3.119.43	142.251.129.132	ICMP	74	Echo (ping) request id=0x0001, seq=154/39424, ttl=128 (reply in 9830)
9830	216.434150	142.251.129.132	10.3.119.43	ICMP	74	Echo (ping) reply id=0x0001, seq=154/39424, ttl=118 (request in 9829)
9852	217.434106	10.3.119.43	142.251.129.132	ICMP	74	Echo (ping) request id=0x0001, seq=155/39680, ttl=128 (reply in 9853)
9853	217.447136	142.251.129.132	10.3.119.43	ICMP	74	Echo (ping) reply id=0x0001, seq=155/39680, ttl=118 (request in 9852)
9872	218.442471	10.3.119.43	142.251.129.132	ICMP	74	Echo (ping) request id=0x0001, seq=156/39936, ttl=128 (reply in 9875)
9875	218.455169	142.251.129.132	10.3.119.43	ICMP	74	Echo (ping) reply id=0x0001, seq=156/39936, ttl=118 (request in 9872)
9907	219.446311	10.3.119.43	142.251.129.132	ICMP	74	Echo (ping) request id=0x0001, seq=157/40192, ttl=128 (reply in 9908)
9908	219.458734	142.251.129.132	10.3.119.43	ICMP	74	Echo (ping) reply id=0x0001, seq=157/40192, ttl=118 (request in 9907)

2. Teste outros filtros, por exemplo, mostre somente pacotes originados e/ou destinados a um determinado host (ip.addr == 192.0.2.1).

The screenshot shows the Wireshark interface with the packet filter `ip.addr == 192.0.2.1` applied. The packet list shows various protocols, including SSDP and HTTP, captured on the 10.3.119.173 interface.

No.	Time	Source	Destination	Protocol	Length	Info
16281	386.131354	10.3.118.173	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16282	386.167756	10.3.118.95	10.3.119.255	UDP	82	62932 → 1947 Len=40
16286	386.397150	10.3.118.25	10.3.119.255	UDP	82	52026 → 1947 Len=40
16287	386.421469	10.3.119.75	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16288	386.438055	10.3.119.42	10.3.119.255	UDP	82	63674 → 1947 Len=40
16289	386.467727	10.3.117.132	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16292	386.716349	10.3.118.68	10.3.119.255	UDP	82	65462 → 1947 Len=40
16296	386.965801	10.3.119.63	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16297	387.023400	10.3.116.131	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16298	387.136711	10.3.118.173	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16300	387.221184	10.3.118.122	10.3.119.255	UDP	82	55145 → 1947 Len=40
16303	387.432731	10.3.119.75	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16304	387.469938	10.3.117.132	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16307	387.556176	10.3.118.119	10.3.119.255	UDP	82	64266 → 1947 Len=40
16311	387.682568	10.3.117.114	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16312	387.682568	10.3.117.114	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16315	387.753078	10.3.117.6	10.3.119.255	UDP	82	56451 → 1947 Len=40
16318	387.996053	10.3.119.82	10.3.119.255	UDP	82	58016 → 1947 Len=40
16322	388.030763	10.3.116.131	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16323	388.050634	10.3.119.194	10.3.119.255	UDP	82	61461 → 1947 Len=40
16325	388.148427	10.3.118.173	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
16334	388.283071	10.3.119.63	10.3.119.255	UDP	82	52947 → 1947 Len=40
16335	388.381703	10.3.118.243	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

3. Qual é o endereço IP do sítio navegador? Qual é o endereço IP da interface de rede do seu computador? Qual o endereço MAC de sua máquina?

Ip do site: Dst: 142.251.129.164

Ip meu: Src: 10.3.119.43,

Mac da minha máquina: Src: Dell\_b4:bf:e5 (d0:94:66:b4:bf:e5)

### **Etapa 3 - Desafio**

```
> Frame 166: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF {3A6069E1-E2F2-4C86-BCB7-0333CCE1005C}, id 0
> Ethernet II, Src: Dell_b4:bf:e5 (d0:94:66:b4:bf:e5), Dst: PaloAlto_1c:a9:30 (5c:58:e6:1c:a9:30) -> MAC
> Internet Protocol Version 4, Src: 10.3.119.43, Dst: 142.251.129.164
> Internet Control Message Protocol
```