Ferramentas básicas: WireShark, Encapsulamento e Tcpdump

1 Verificando pacotes do ping (ICMP REQUEST/REPLY)

1.1 Aplique um filtro icmp no display. Recorte a tela observada e indique os pacotes ICMP ECHO REQUEST. Anote quem são os endereços IP e MAC que aparecem no pacote IP e Frame Ethernet.

Em azul, estão listados os pacotes ICMP ECHO REQUEST, pacote No. **39**, **43** e **46**. O endereço IP de origem é **192.168.0.4** e de destino **191.36.0.94**. O endereço MAC de origem é **ec:63:d7:7d:3b:f1** e de destino **cc:58:30:01:87:c5**.

Figura 1: Solicitações e respostas ao envio de pacotes.

No.	Time	Source	Destination	Protocol	Length	Info
39	25.300469290	192.168.0.4	191.36.0.94	ICMP	98	Echo (ping) request id=0xadb1, seq=1/256, ttl=64 (reply in 40)
40	25.324068937	191.36.0.94	192.168.0.4	ICMP	98	Echo (ping) reply id=0xadb1, seq=1/256, ttl=55 (request in 39)
43	26.302257267	192.168.0.4	191.36.0.94	ICMP	98	Echo (ping) request id=0xadb1, seq=2/512, ttl=64 (reply in 44)
44	26.325399917	191.36.0.94	192.168.0.4	ICMP	98	Echo (ping) reply id=0xadb1, seq=2/512, ttl=55 (request in 43)
46	27.303017111	192.168.0.4	191.36.0.94	ICMP	98	Echo (ping) request id=0xadb1, seq=3/768, ttl=64 (reply in 47)
47	27.330856984	191.36.0.94	192.168.0.4	ICMP	98	Echo (ping) reply id=0xadb1, seq=3/768, ttl=55 (request in 46)

Fonte: Elaborada pela autora.

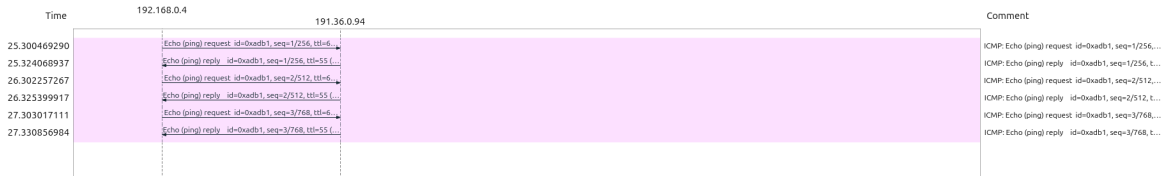
Figura 2: Verificando o pacote 39 de solicitação.

```
▸ Frame 39: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
▸ Ethernet II, Src: Intel_7d:3b:f1 (ec:63:d7:7d:3b:f1), Dst: SagemcomBroa_01:87:c5 (cc:58:30:01:87:c5)
▸ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 191.36.0.94
▸ Internet Control Message Protocol
```

Fonte: Elaborada pela autora.

1.2 Aplique um comando Flow Graph e mostre a troca de mensagens do ping através de um recorte da tela. Statistics » Flow Graph » Abrirá uma nova janela com várias informações » Aplique o filtro (Flow type:) ICMP Flows na base da janela. Salve esta tela no relatório. Feche esta janela.

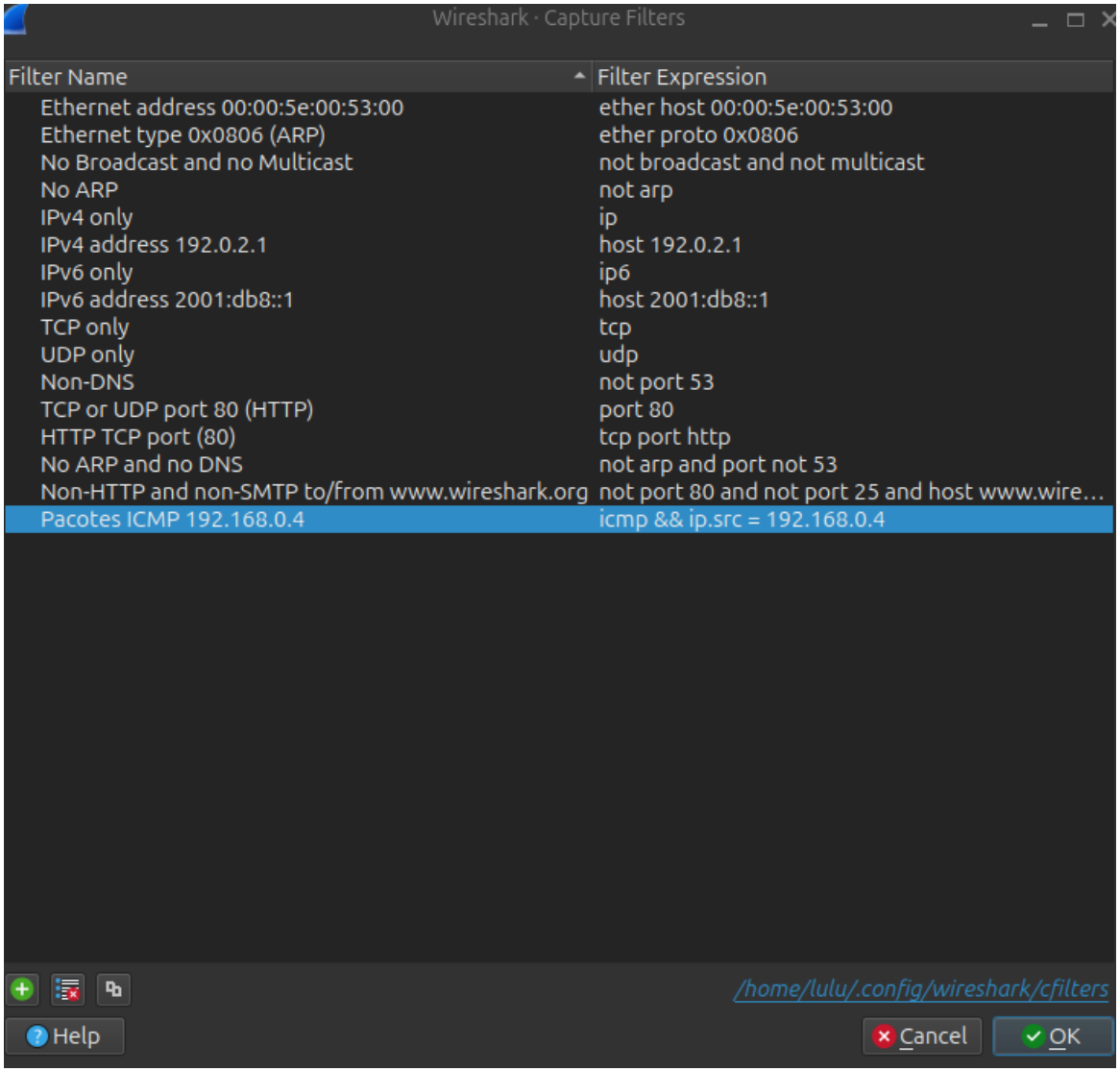
Figura 3: Painel Flow Graph.



Fonte: Elaborada pela autora.

1.3 Crie um filtro para mostrar somente pacotes ICMP que saem da sua máquina (ver filtro `ip.src`). Faça um recorte das telas de criação do filtro (mostrando o filtro).

Figura 4: Criando filtro para pacotes ICMP que saem da máquina.

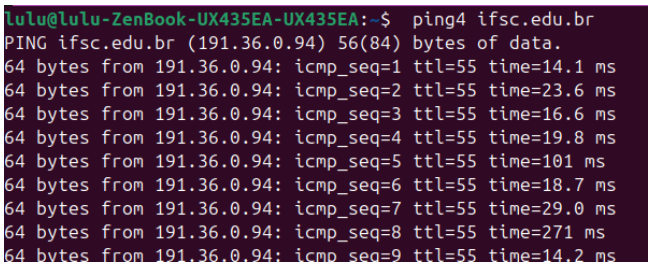


Fonte: Elaborada pela autora.

2 Tcpdump

2.1 Abra um terminal e faça um ping

Figura 5: Exemplo de comando ping executado no terminal.

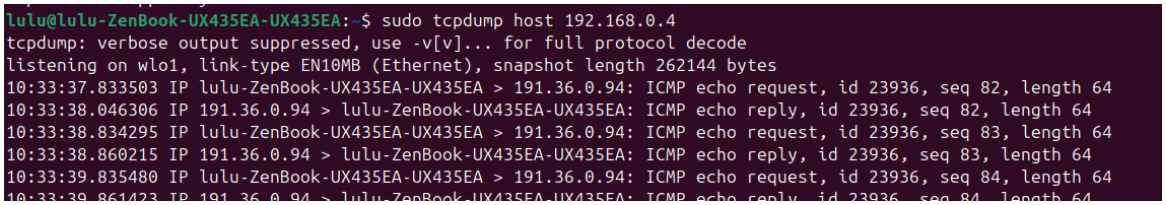


Fonte: Elaborada pela autora.

2.2 Abra outro terminal e faça um tcpdump e, com o uso de parâmetros (filtros) apropriados, faça com que o tcpdump mostre:

2.2.1 Capture todos os pacotes oriundos e destinados à sua máquina.

Figura 6: Captura de pacotes sem flags adicionais.

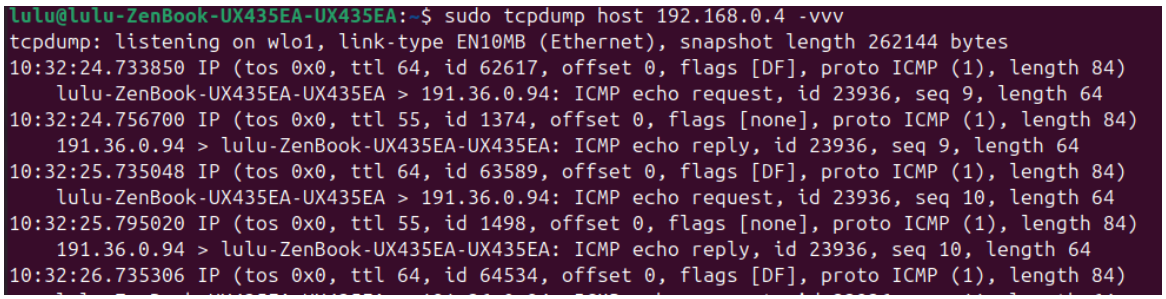


Fonte: Elaborada pela autora.

2.2.2 Idem anterior com a flag -vvv ativa e, em seguida, a flag -n. Qual é a função dessas flags?

A flag -vvv aumenta o detalhamento exibido na saída dos pacotes, ou seja, aumenta a chamada "verbosidade", e a flag -n não converte endereços, ou seja, ela não exibe o nome de hosts e números de portas.

Figura 7: Captura com a flag `-vvv` ativada.



Fonte: Elaborada pela autora.

Figura 8: Captura com a flag `-n` ativada.

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ sudo tcpdump host 192.168.0.4 -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:33:08.790825 IP 192.168.0.4 > 191.36.0.94: ICMP echo request, id 23936, seq 53, length 64
10:33:08.822987 IP 191.36.0.94 > 192.168.0.4: ICMP echo reply, id 23936, seq 53, length 64
10:33:09.792368 IP 192.168.0.4 > 191.36.0.94: ICMP echo request, id 23936, seq 54, length 64
10:33:09.826059 IP 191.36.0.94 > 192.168.0.4: ICMP echo reply, id 23936, seq 54, length 64
```

Fonte: Elaborada pela autora.

2.2.3 Capture somente os pacotes oriundos de sua máquina. Anote o comando utilizado.

```
sudo tcpdump host 192.168.0.4 -Q out
```

Figura 9: Captura de pacotes oriundos da máquina.

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ sudo tcpdump host 192.168.0.4 -Q out
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:36:29.163491 IP lulu-ZenBook-UX435EA-UX435EA > 191.36.0.94: ICMP echo request, id 23936, seq 253, length 64
10:36:29.187961 IP lulu-ZenBook-UX435EA-UX435EA.45409 > 239.255.255.250.1900: UDP, length 172
10:36:29.637404 IP lulu-ZenBook-UX435EA-UX435EA.48012 > 150.138.117.34.bc.googleusercontent.com.https: Flags [.], a
847], length 0
10:36:30.165463 IP lulu-ZenBook-UX435EA-UX435EA > 191.36.0.94: ICMP echo request, id 23936, seq 254, length 64
10:36:30.189188 IP lulu-ZenBook-UX435EA-UX435EA.45409 > 239.255.255.250.1900: UDP, length 172
10:36:31.167582 IP lulu-ZenBook-UX435EA-UX435EA > 191.36.0.94: ICMP echo request, id 23936, seq 255, length 64
```

Fonte: Elaborada pela autora.

2.2.4 Capture somente pacotes destinados à sua máquina. Anote o comando utilizado.

```
sudo tcpdump host 192.168.0.4 -Q in
```

Figura 10: Captura de pacotes destinados à máquina.

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ sudo tcpdump host 192.168.0.4 -Q in
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:36:11.156190 IP 191.36.0.94 > lulu-ZenBook-UX435EA-UX435EA: ICMP echo reply, id 23936, seq 235, length 64
10:36:12.178222 IP 191.36.0.94 > lulu-ZenBook-UX435EA-UX435EA: ICMP echo reply, id 23936, seq 236, length 64
10:36:13.172289 IP 191.36.0.94 > lulu-ZenBook-UX435EA-UX435EA: ICMP echo reply, id 23936, seq 237, length 64
10:36:14.157741 IP 191.36.0.94 > lulu-ZenBook-UX435EA-UX435EA: ICMP echo reply, id 23936, seq 238, length 64
10:36:15.164778 IP 191.36.0.94 > lulu-ZenBook-UX435EA-UX435EA: ICMP echo reply, id 23936, seq 239, length 64
10:36:16.255493 IP 191.36.0.94 > lulu-ZenBook-UX435EA-UX435EA: ICMP echo reply, id 23936, seq 240, length 64
^C
```

Fonte: Elaborada pela autora.

2.3 Repita os comandos acima e, com o uso de parâmetros apropriados, faça com que o tcpdump armazene os dados em um arquivo denominado “pacotes_capturadosX.pcap“ (um arquivo para cada item acima, onde X é o número do item). Anote os comandos no relatório.

```
sudo tcpdump host 192.168.0.4 -w "pacotes_capturados1.pcap"
```

Captura de pacotes oriundos e destinados à sua máquina.

```
1 sudo tcpdump host 192.168.0.4 -vvv -w "pacotes_capturados2.1.pcap"
```

Captura de pacotes é apresentada com maior verbosidade.

```
1 sudo tcpdump host 192.168.0.4 -n -w "pacotes_capturados2.2.pcap"
```

Captura de pacotes é apresentada sem a conversão de endereços.

```
1 sudo tcpdump host 192.168.0.4 -Q out -w "pacotes_capturados3.pcap"
```

Captura de pacotes somente oriundos da máquina.

```
1 sudo tcpdump host 192.168.0.4 -Q in -w "pacotes_capturados4.pcap"
```

Captura de pacotes somente destinados à máquina.

2.4 Procure um dos arquivos salvos, com o navegador de arquivos de sua máquina, dê um duplo clique sobre o mesmo.

O programa aberto foi o Wireshark.