Atividade Pratica: Analise de Protocolo com Wireshark

-Bernardo Rizzone (232013194)

PARTE 3:

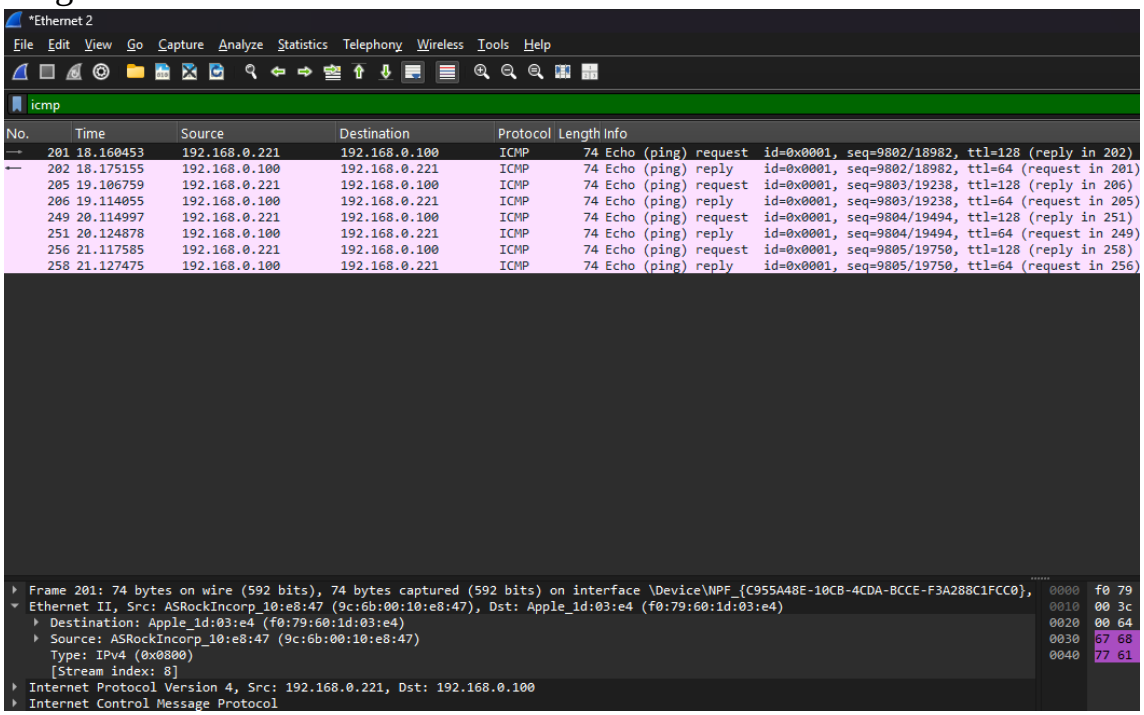
Meu computador:

```
Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller #2
Endereço Físico . . . . . . . . . . . . . : 9C-6B-00-10-E8-47
DHCP Habilitado . . . . . . . . . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 . . . . . . . . . . . : 2804:14c:6584:4d58::1000(Preferencial)
Concessão Obtida. . . . . . . . . . . . . : terça-feira, 2 de setembro de 2025 16:45:34
Concessão Expira. . . . . . . . . . . . . : quarta-feira, 3 de setembro de 2025 15:28:35
Endereço IPv6 . . . . . . . . . . . : 2804:14c:6584:4d58:383d:cab5:d324:bd0b(Preferencial)
Endereço IPv6 Temporário. . . . . . . . . : 2804:14c:6584:4d58:78bb:d824:e11b:98f3(Preferencial)
Endereço IPv6 de link local . . . . . . . . : fe80::37db:7233:48fb:17aa%18(Preferencial)
Endereço IPv4. . . . . . . . . . . . . . . : 192.168.0.221(Preferencial)
```

Computador Analisado:

```
options=400<CHANNEL_IO>
ether f0:79:60:1d:03:e4
inet6 fe80::1c7b:41ee:bb79:8631%en0 prefixlen 64 secured scopeid 0x4
inet6 2804:14c:6584:4d58:18bc:44fe:f51c:c23f prefixlen 64 autoconf secured
inet6 2804:14c:6584:4d58:ad00:ca60:14f2:2be9 prefixlen 64 autoconf temporary
inet6 2804:14c:6584:4d58::1000 prefixlen 64 dynamic
inet 192.168.0.100 netmask 0xffffff00 broadcast 192.168.0.255
```

Ping no wireshark:

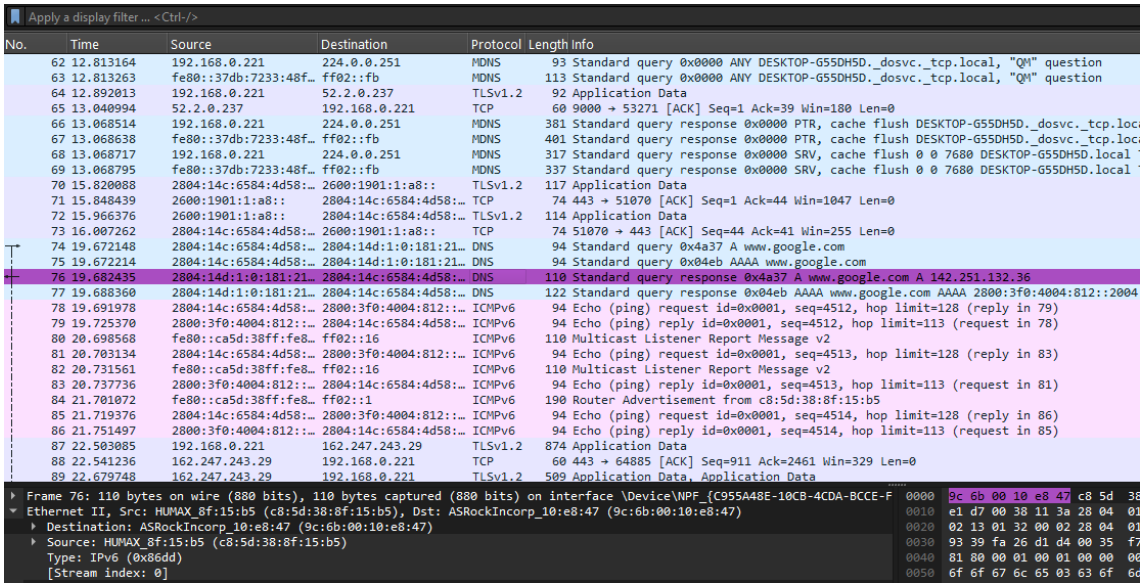


Ambos os endereços MAC correspondem aos devidos computadores.

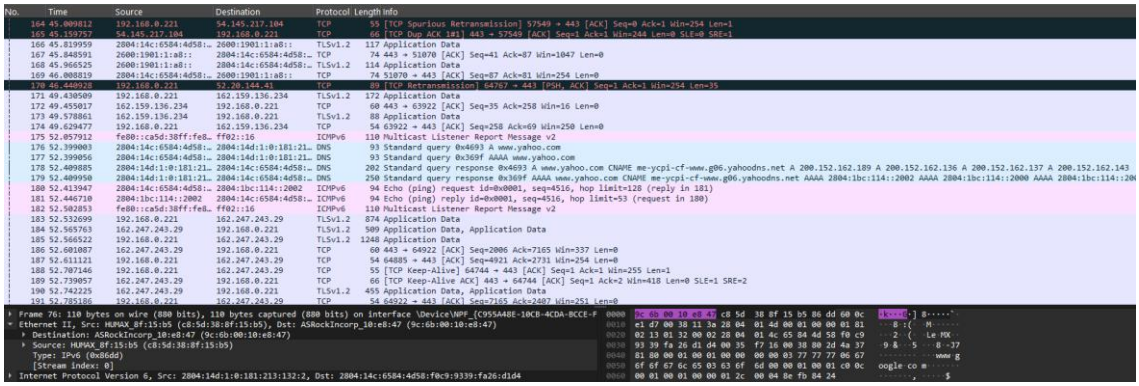
PARTE 3:

Local	Endereço de IP de Destino	Endereço Mac de Destino
Yahoo	200.152.162.189	c8:5d:38:8f:15:b5
Cisco		c8:5d:38:8f:15:b5
Google	142.251.132.36	c8:5d:38:8f:15:b5

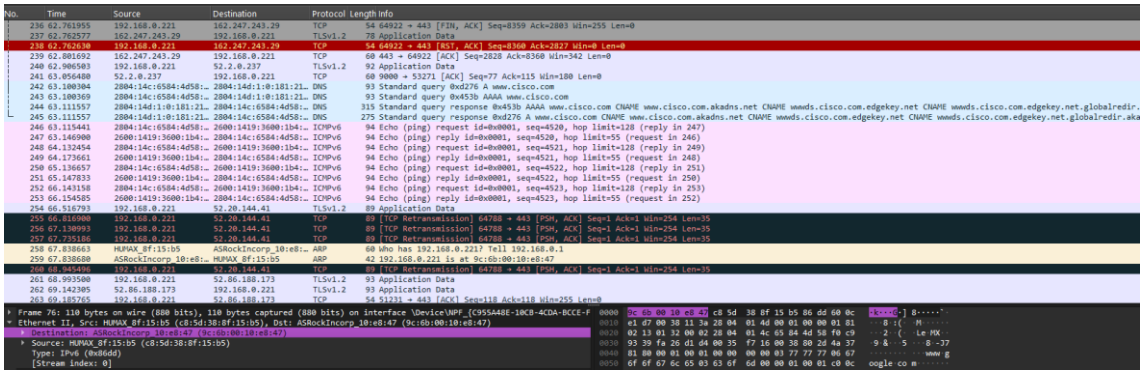
Imagens de analise: Google



Yahoo:



Cisco:



Ping do cisco no DNS não apareceu o ipv4 nem o ipv6.

Questões dissertativas:

1. **Na Parte 2, como o seu computador descobriu o endereço MAC do outro computador?**

R: Meu computador descobriu o endereço MAC do outro computador usando o Protocolo ARP. Ao tentar enviar o ping, ele primeiro enviou uma mensagem ARP em broadcast para toda a rede loca, perguntando: “Quem tem este endereço IP?”. O outro computador respondeu diretamente com seu endereço MAC. Após receber essa resposta, meu computador armazenou essa informação e utilizou o endereço MAC recebido para enviar os pacotes de ping.

2. **Na parte 3, os endereços MAC de destino que você anotou pertencem aso servidores da Cisco, Google , e Yahoo? Se não, a qual dispositivo eles pertencem? Qual a importância dessa informação?**

R: Não, esse endereço MAC não pertence aos servidores do google, yahoo e cisco. Ele pertence ao meu roteador, que atua como o gateway padrão da rede local para a internet. A importância dessa informação demonstra a diferença entre o endereçamento local e o endereçamento global. O endereço MAC e usado para a entrega local, ou seja, para encontrar o próximo dispositivo no caminho dentro da sua propia rede. No caso, para sair para a internet, o roteador e usando como “Ponte”.

3. **Comparando os resultados da parte 2 e da parte 3, explique por que o wireshark exibe o endereço MAC real do host de destino para pings locais, mas não para pings remotos.**

R: Para os pings locais (Parte 2), o computador de destino está na mesma rede que o meu. Isso significa que eles podem se comunicar diretamente. Meu computador utiliza o protocolo ARP para obter o endereço MAC específico do host de destino e, em seguida, cria um quadro Ethernet endereçado diretamente do meu MAC para o MAC do

outro computador. Para os pings remotos (Parte 3), o host de destino (como o Google) está em uma rede externa. O endereço MAC só tem validade dentro da nossa rede local e não pode ser usado para roteamento na internet. Meu computador, ao perceber que o IP de destino é externo, envia o pacote para o seu gateway padrão, que é o nosso roteador.