**Ficha de trabalho Nº1 - ICMP**

**1-**Os RFCs são documentos individualmente numerados e publicados em serie.

São feitos e revistos por um grupo de engenheiros, de forma a descrever métodos, comportamentos e inovações de um protocolo. Os documentos são vistos como Padrões da Internet.

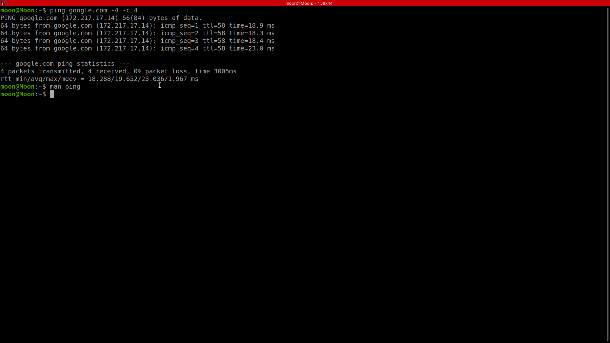
Uma vez que o documento recebe um número e é publicado, não pode ser retirado nem modificado. Se o documento precisar de ser alterado, os autores têm que publicar um novo documento revisado.

**2-** O Internet Protocol (IP) é usado para host-to-host de datagrama em um sistema de redes interconectadas chamado Catenet. Os gateways se comunicam entre si para fins de controle por meio de um Gateway to Gateway Protocol (GGP). Um gateway irá se comunicar com um host de origem para assim poder relatar um erro no processamento do datagrama. Para tal, utiliza-se o protocolo, Internet Control Message Protocol (ICMP).

As mensagens ICMP são enviadas em várias situações como por exemplo, quando o datagrama não pode alcançar seu destino, etc. O IP não foi feito para ser totalmente confiável, pois o objetivo dessas mensagens de controlo é dar um feedback sobre problemas no ambiente de comunicação.

As mensagens ICMP geralmente relatam erros no processamento de

datagramas.

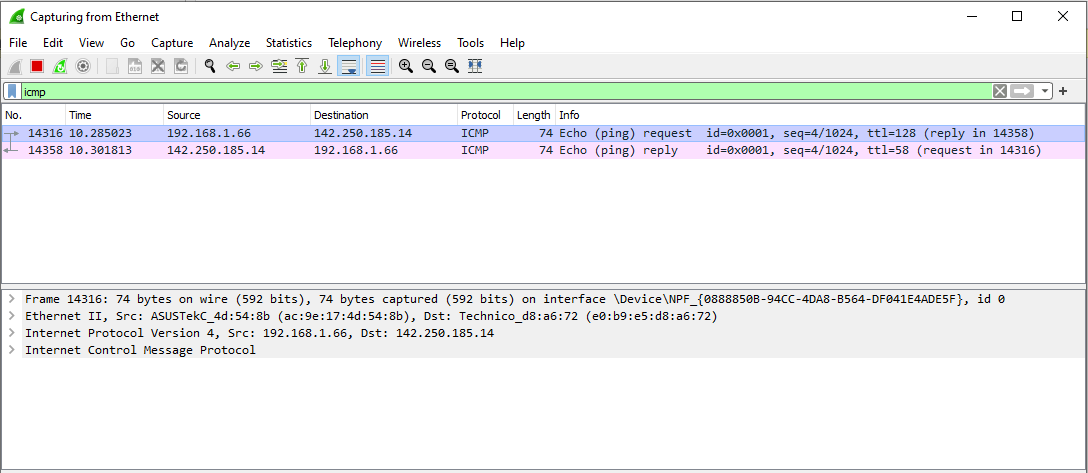
**3-** Na seguinte imagem, executei o commando "ping google.com", usando o protocolo ICMP mandei um "ECHO\_REQUEST" com o objetivo de receber um "ECHO\_RESPONSE" do site para saber se o site estava ativo. Obtivemos uma resposta do site, indicando que ele estava a ativo e pronto a receber pacotes ICMP. Nao houve qualquer perda de pacotes. O round trip time (RTT) medio foi de 18.288ms. O time to live (ttl) de cada pacote era de 58ms.

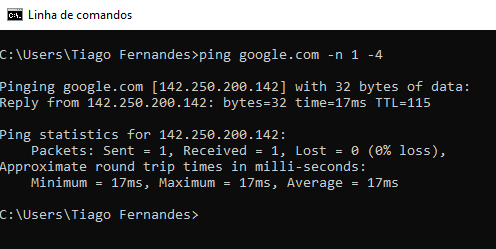
**4-** O wireshark é um programa que analisa o tráfego de rede e que organiza este por protocolos. Através deste programa consegue-se controlar o tráfego de uma rede e monitorar a entrada e saída de dados do computador, em vários protocolos diferenciados, ou até mesmo da rede à qual o computador está ligado.

Também é possível o tráfego de um dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos.

**5-** No cabecalho do wireshark vemos que foram capturados dois pacotes de informacao usando o protocolo ICMP. O primeiro foi um "ECHO\_REQUEST"

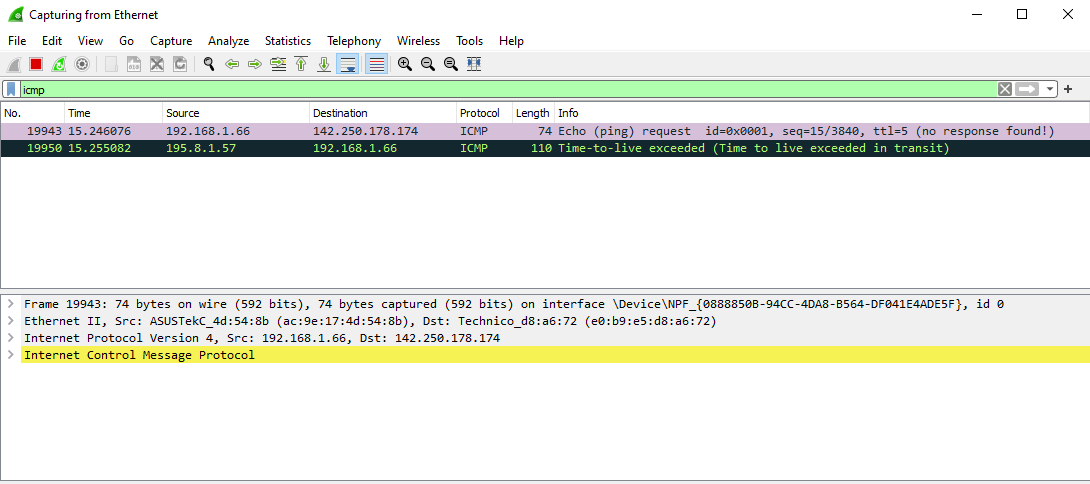
que nos mandamos para o destinatario (142.250.178.174) O segundo foi um "ECHO\_REPLY" que o site mandou de volta para nos (192.168.1.95).

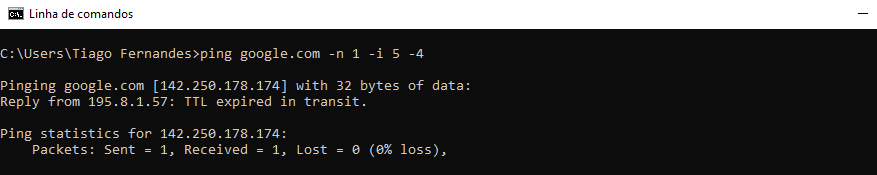




**7-** Estabelecemos a conexão com o destinatário (142.250.178.174) onde enviámos um pacote ICMP (echo request) com um TTL de 5 saltos.

Recebemos uma resposta do destinatário com um pacote ICMP com 32 bytes e também sem qualquer perda do mesmo.





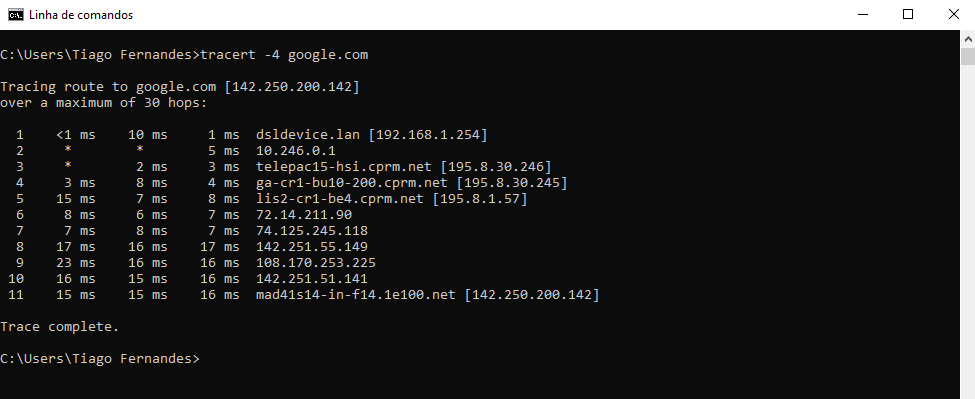
**8-** O comando traceroute é uma ferramenta de diagnóstico usada para rastrear os pacotes de ICMP e reporta o ip de cada nó que o mesmo passa.

Tentamos estabelecer uma conexão com o destinatário (google.com) através do protocolo ICMP e observamos que o pacote passou por 11 nós até chegar ao seu destino.

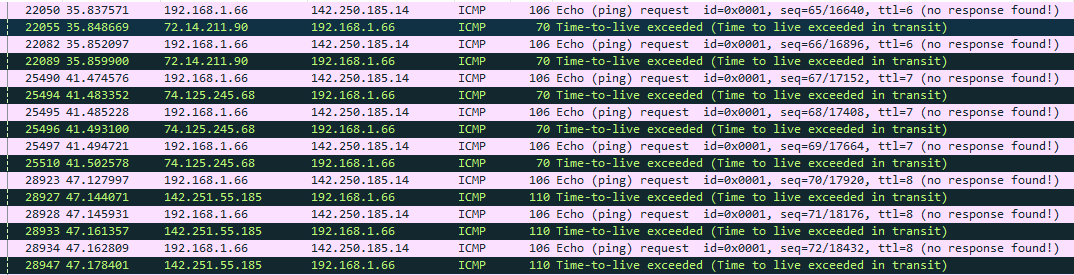
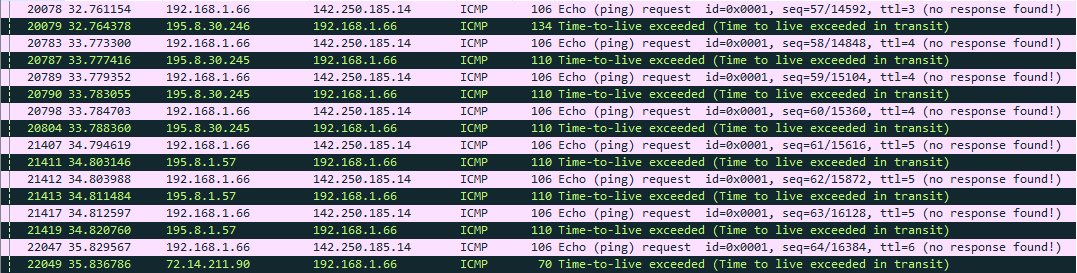
A 1º coluna aponta os saltos que o pacote fez.

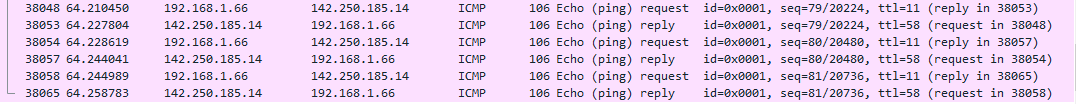
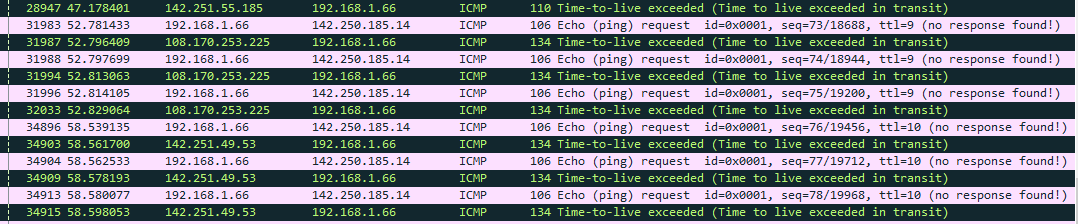
As próximas 3 colunas indicam o RTT (Round Trip Time) para o nosso pacote chegar ao destino e obtermos uma resposta.

A última coluna mostra-nos os IPs dos nós em que o pacote passa e se estiver disponível usa o domain name.

Os “\*” significa que possa ter ocorrido uma mensagem perdida. 

**9-** Verificámos que enviámos 3 pacotes por cada nó. Na imagem do cmd os “\*” são pacotes que não tivemos resposta de volta. A cada nó que passa vamos aumentando o TTL (time to live), este começando no 1 com o objetivo de terminar o TTL necessário para chegar ao destino (TTL=0).





**10-** Em suma, o propósito do protocolo ICMP é para reportar erros e fazer diagnósticos a redes. Este ajuda na comunicação entre dois dispositivos pela internet de forma segura e de fácil entendimento.