Exercícios Wireshark – ICMP

Primeira parte: Escolha um **site** e realize o seguinte comando ping: **ping -n 10 www.site.com.br.** Logo após a execução do comando ping execute a captura de dados somente do protocolo ICMP e responda às perguntas de 1 a 4 a seguir:

1.Qual é o endereço IP da sua máquina? Qual é o endereço IP da máquina destino?

2. Por que um pacote ICMP não tem números de porta de origem e destino?

3. Examine um dos pacotes de solicitação de ping enviados pela sua máquina. Quais são o tipo de ICMP e os números de código? Que outros campos esse pacote ICMP possui? Quantos bytes são os campos de soma de verificação, número de sequência e identificador?

4. Examine o pacote de resposta de ping correspondente. Quais são o tipo de ICMP e os números de código? Que outros campos esse pacote ICMP possui? Quantos bytes são os campos de soma de verificação, número de sequência e identificador?

Segunda parte: Escolha um **site** e realize o seguinte comando traceroute: **traceroute www.site.com.br.** Logo após a execução do comando traceroute execute a captura de dados até o término da execução do comando, e responda às perguntas de 5 a 10 a seguir:

5. Qual é o endereço IP da sua máquina? Qual é o endereço IP da máquina destino?

6. Se o ICMP enviasse pacotes UDP (como no Unix/Linux), o número do protocolo IP ainda seria 01 para os pacotes de teste? Se não, o que seria?

7. Examine o pacote de eco ICMP na captura de tela. Isso é diferente dos pacotes de consulta de ping ICMP na primeira parte desses exercícios? Se sim, o que há de diferente?

8. Examine o pacote de erro ICMP na captura de tela. Tem mais campos do que o pacote de eco ICMP. O que está incluído nesses campos?

9. Examine os últimos três pacotes ICMP recebidos pela máquina origem. Como esses pacotes são diferentes dos pacotes de erro ICMP? Por que eles são diferentes?

10. Nas medições do traceroute, existe um link cujo atraso é significativamente maior do que outros? Consulte a captura de tela e veja se há um link cujo atraso é significativamente maior do que outros? Com base nos nomes dos roteadores, você consegue adivinhar a localização dos dois roteadores no final deste link?