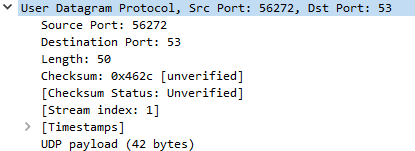
**ANÁLISE DO PROTOCOLO UDP**

Para as respostas abaixo foi utilizado o pacote nº 1 do arquivo disponibilizado para download no material online.

1. Selecione um pacote UDP de sua captura. A partir desse pacote, determine quais campos existem no cabeçalho UDP. Responda a essas perguntas observando diretamente o pacote capturado. Nomeie esses campos.

No campo “lista de pacotes” da janela principal do Wireshark expanda a entrada “User Datagram Protocol”. Deverá aparecer algo como:

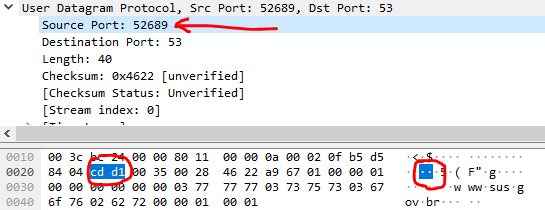


Pela imagem é possível observar 4 campos:

* Source port (porta origem)
* Destination port (porta destino)
* Length (tamanho)
* Checksum (soma de verificação)

2. Consultando as informações exibidas no campo “conteúdo do pacote” do Wireshark para este pacote, determine o comprimento (em bytes) de cada um dos campos do cabeçalho UDP.

Clicando em cada cabeçalho no campo “lista de pacotes”, seu conteúdo é iluminado no campo “conteúdo do pacote”. Vendo a quantidade de bytes iluminados é possível determinar o tamanho de cada cabeçalho. Na imagem abaixo é selecionado o cabeçalho “source port”, e são iluminados 2 bytes. Portanto esse cabeçalho possui 2 bytes.



Respostas:

* Source port: 2 bytes
* Destination port: 2 bytes
* Length: 2 bytes
* Checksum: 2 bytes

3. O valor do campo de cabeçalho “Tamanho” é o tamanho de quê? Qual o valor deste campo para o pacote capturado? Com base nessa informação, quantos bytes de dados são carregados nesse segmento UDP?

É o tamanho do segmento em bytes incluindo o cabeçalho.

Para o pacote capturado o campo de cabeçalho tem valor 40 (40 bytes).

Como o segmento UDP possui tamanho 40 bytes e seu cabeçalho possui 8 bytes, esse segmento UDP carrega 32 bytes de dados.

4. Qual é a quantidade máxima de bytes que podem ser incluídos em uma carga útil UDP?

O campo de cabeçalho “Tamanho” possui 16 bits, então pode conter até o valor 216-1 = 65535.

Retirando os 8 bytes do cabeçalho e desprezando limitações impostas pelas camadas inferiores cada segmento UDP poderia em teoria carregar ate 65527 byes.

5. Qual é o maior número de porta de origem possível?

Como o campo de cabeçalho “porta origem” possui 16 bits, então pode conter até o valor 216-1 = 65535.

6. Em que porta a aplicação está aguardando pelos dados desse segmento no hospedeiro destino?

O valor do campo de cabeçalho “porta destino” desse segmento é 53, portanto a aplicação no destino está aguardando por mensagens na porta 53.

7. Esse segmento está enviando algum código para verificação de erros? Como foi possível determinar isso?

Sim. Quando o UDP não envia código para verificação de erros o valor do campo de cabeçalho “checksum” é zero. Como o valor do checksum nesse segmento é 0x4622 então a origem está enviando valor para que o destino possa verificar se a mensagem chegou íntegra.