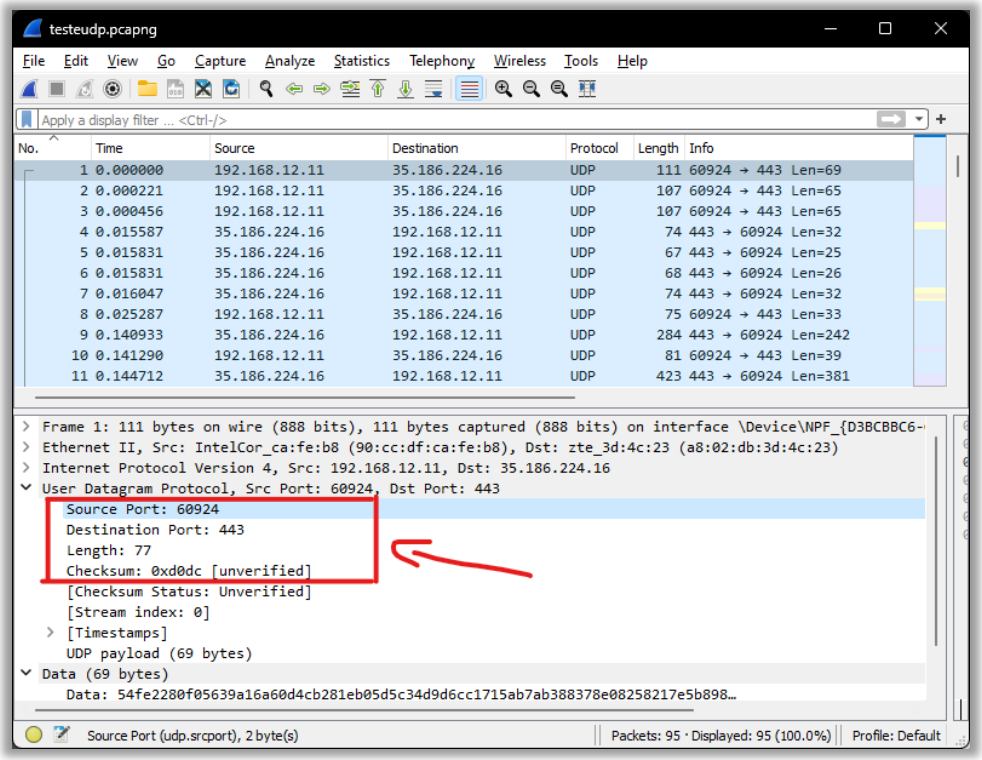
WireShark Lab 04 - UDP v7.0

Igor Augusto Reis Gomes – 12011BSI290 – igor.augusto@ufu.br

Heitor Guimarães Da Fonseca Filho – 12011BSI203 – heitor.filho@ufu.br

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields

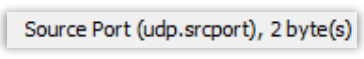
Há 4 quatro campos no cabeçalho: source port (porta de origem), destination port (porta de destino), length (comprimento) e checksum (soma de verificação).

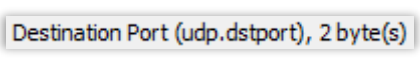


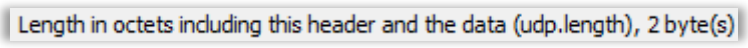
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Como é possível observar nos prints abaixo, todos os quatro campos do cabeçalho UDP possuem tamanho de 2 bytes, possível de ser observado no rodapé da janela do aplicativo.

Segue abaixo os campos source port, destination port, length e checksum, respectivamente:

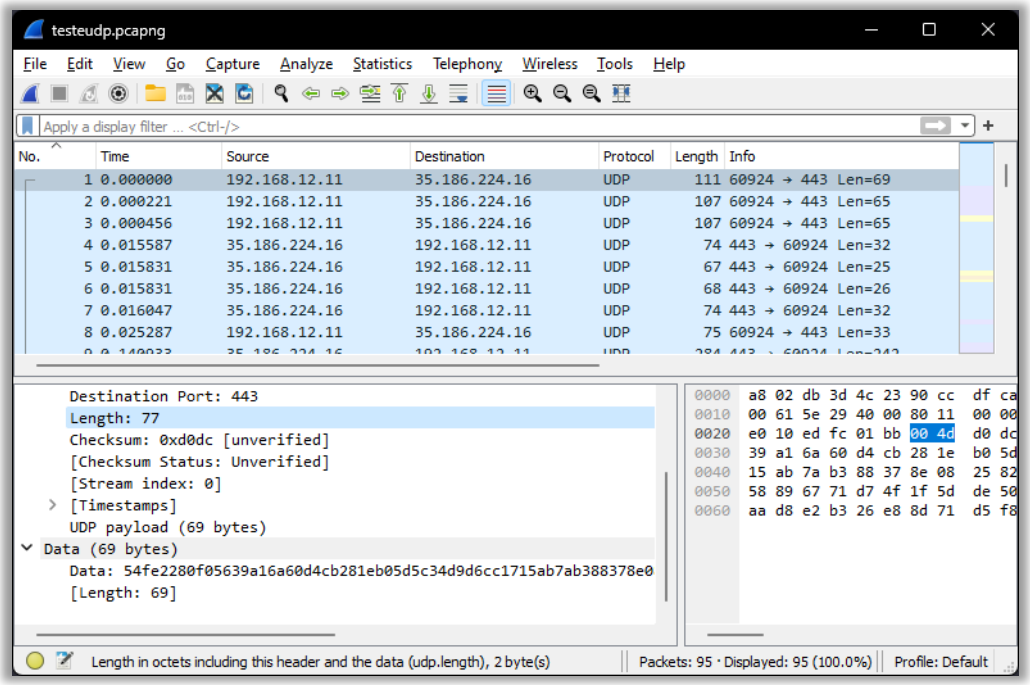






3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

O campo "length" no cabeçalho de um pacote UDP indica o tamanho total do pacote, incluindo cabeçalho e dados. Dado o pacote abaixo com um valor de "length" igual a 77, o cabeçalho UDP contribui com 8 bytes (4 campos de 2 bytes cada), deixando 69 bytes para os dados contidos no pacote UDP.



4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

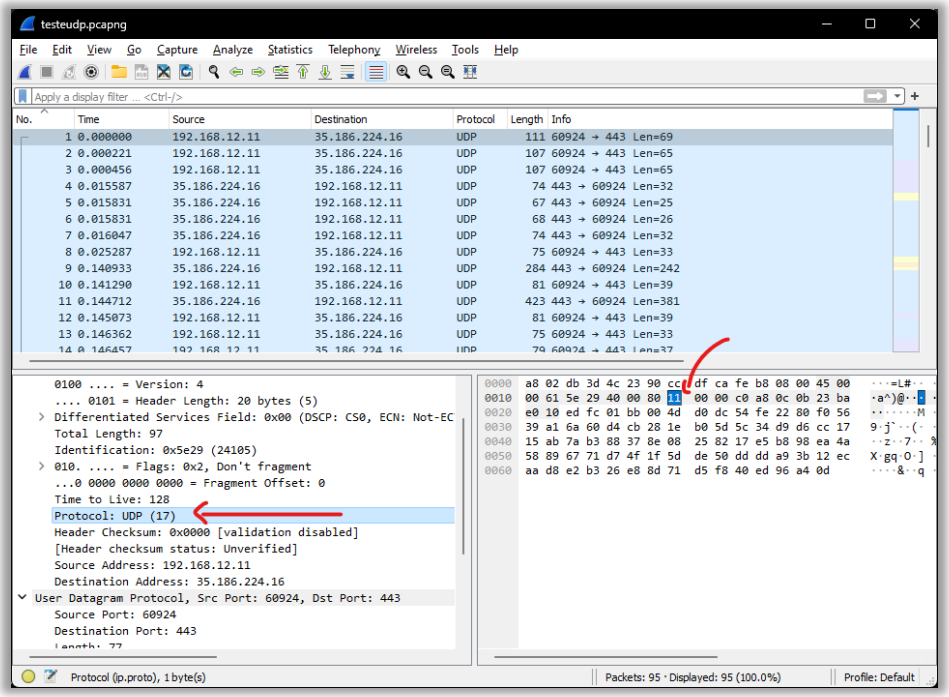
Neste caso, o maior número de porta de origem possível é (2^16 – 1) = 65535. Sendo que 2^16 (65536) é o número máximo que pode ser representado com 16 bits. Dessa forma, considerando que cabeçalho tem tamanho de 8 bytes, subtraímos essa quantia no cálculo, resultando em uma carga útil máxima do UDP de 65535 – 8 = 65527 bytes.

5. What is the largest possible source port number? (Hint: see the hint in 4.)

Com apenas 16 bits, a maior porta de origem possível é a de número (2^16 – 1) = 65535.

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

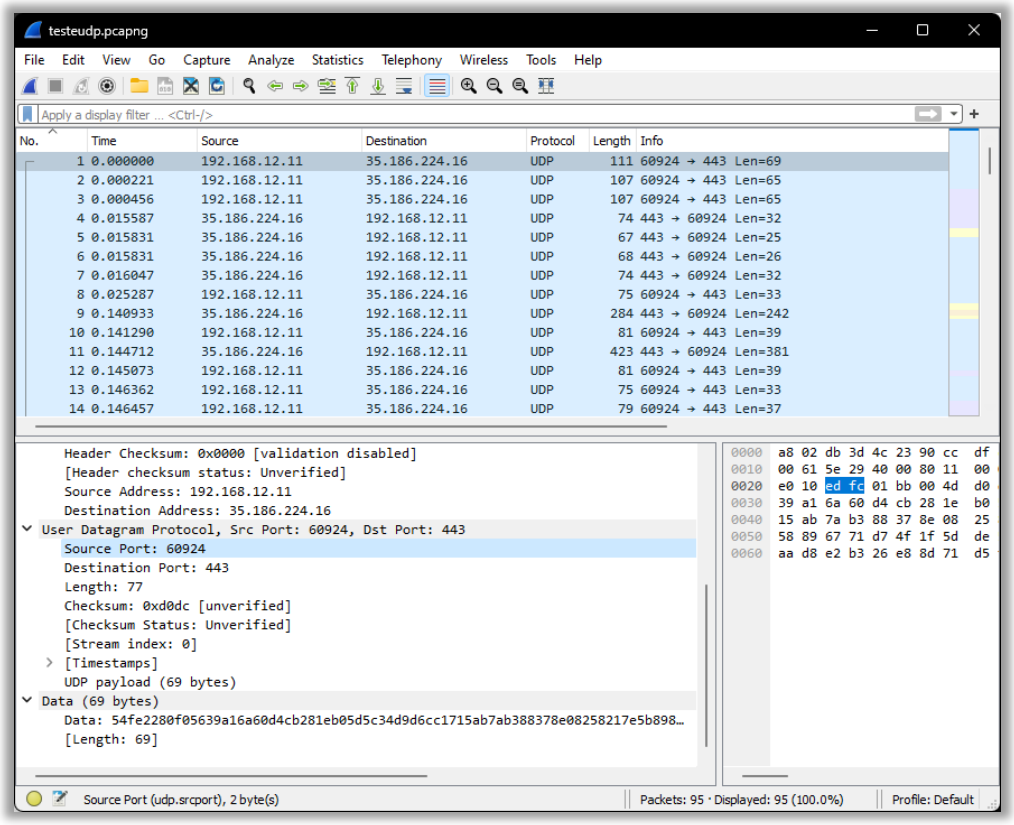
O número de protocolo do UDP é 17 (em decimal) e 11 (em hexadecimal), como é possível ser observado indicado abaixo:



7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

Como é possível observar nos prints abaixo (na próxima página), o número da porta de origem do pacote de requisição (envio) é o mesmo da porta de destino do pacote de resposta, isto é, 60924. Da mesma forma, o número da porta de origem de resposta é o mesma que o da porta de destino da requisição (envio), isto é, a 443.

Pacote UDP de requisição (envio)



Pacote UDP de resposta