Atividade 2 – Wireshark - Captura FTP (Modificado)

1. Nome: Igor Correa RA: 15.00588-7  
   Nome: Rodrigo Franciozi RA: 14.04014-0  
   Nome: RA:
2. Topologia (FTP)

A parte 1 destacará uma captura TCP de uma sessão FTP. Essa topologia consiste em um computador com acesso à Internet.



1. Objetivos

Parte 1: Identificar os campos do cabeçalho e a operação TCP usando uma captura de sessão FTP do Wireshark

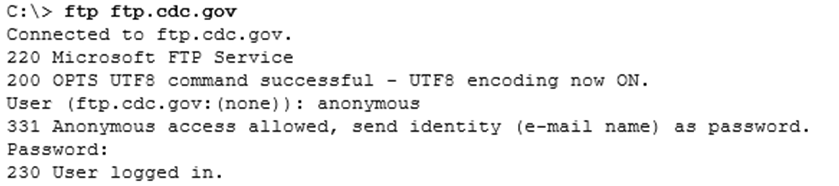
1. Recursos Necessários – Parte 1 (FTP)

1 PC (com Windows com acesso ao prompt de comando, acesso à Internet e Wireshark instalado)

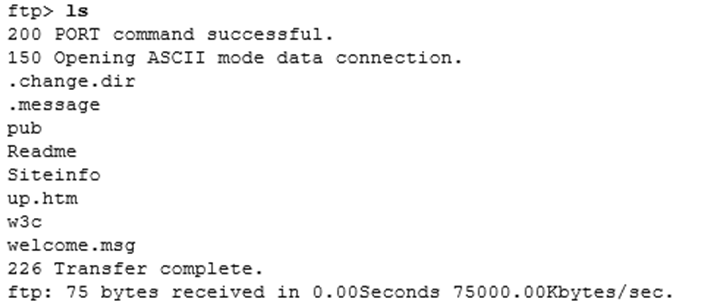
1. Identificar os Campos do Cabeçalho e a Operação TCP Usando uma Captura de Sessão FTP do Wireshark

Na Parte 1, use o Wireshark para capturar uma sessão FTP e inspecionar os campos do cabeçalho TCP.

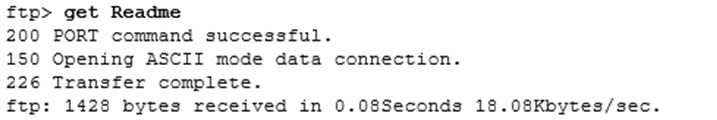
* 1. Iniciar uma captura do Wireshark.
     1. Feche todo o tráfego de rede desnecessário, como por exemplo, o navegador Web, para limitar a quantidade de tráfego durante a captura do Wireshark.
     2. Inicie a captura do Wireshark.
  2. Baixar o arquivo Readme (Leiame).
     1. No prompt de comandos, insira **ftp ftp.cdc.gov**.
     2. Efetue login no site FTP do Centro de Controle e Prevenção de Doenças (CDC) com o usuário **anonymous** e nenhuma senha.



* + 1. Digite o comando Is para listar os arquivos, em seguida, localize e baixe o arquivo Readme (Leiame).

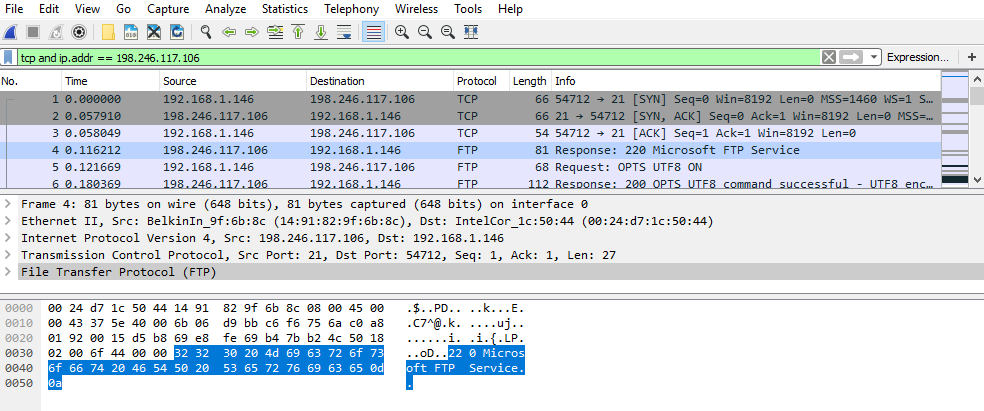


* + 1. Digite o comando **get Readme** para baixar o arquivo. Quando o download do arquivo estiver completo, digite o comando quit para sair.



* 1. Parar a captura do Wireshark.
  2. Exibir a janela principal do Wireshark.

O Wireshark capturou muitos pacotes durante a sessão FTP com ftp.cdc.gov. Para limitar a quantidade de dados para análise, digite **tcp and ip.addr == 198.246.117.106** na área **Filter: entry** e pressione **Enter**. O endereço IP, 198.246.117.106, é o endereço de [ftp.cdc.gov](ftp://ftp.cdc.gov) no momento da criação deste laboratório.



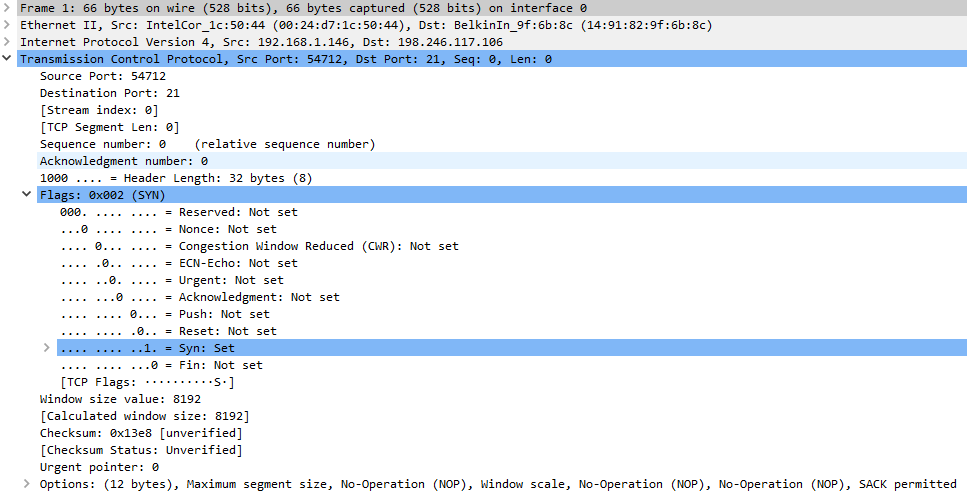
* 1. Analisar os campos TCP.

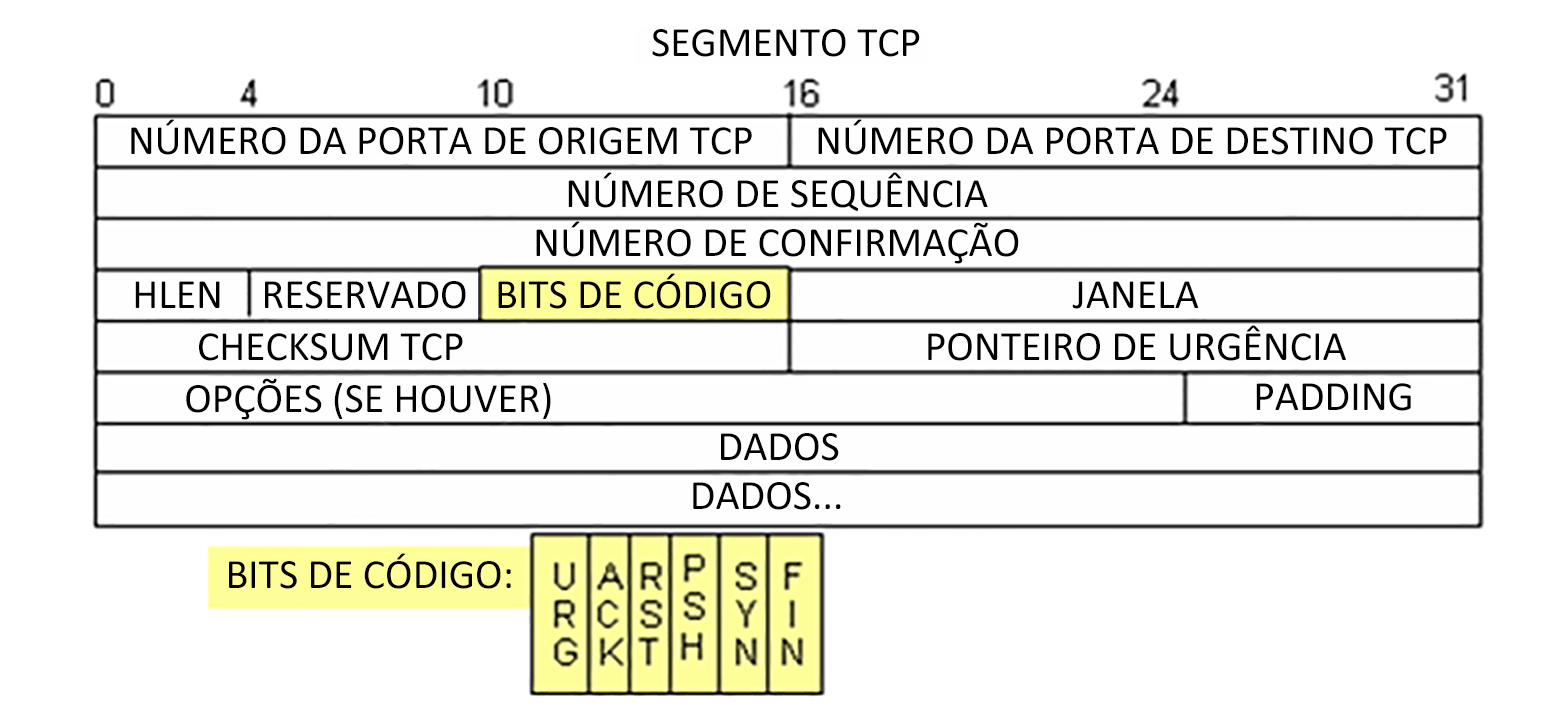
Depois do filtro TCP ter sido aplicado, os primeiros três quadros no painel de lista de pacotes (seção superior) exibem o protocolo TCP de camada de transporte que cria uma sessão segura. A sequência [SYN], [SYN, ACK], e [ACK] ilustra o handshake triplo.



O TCP é comumente usado durante uma sessão para controlar a entrega de datagramas, verificar a chegada de datagramas e gerenciar o tamanho da janela. Em cada troca de dados entre o cliente FTP e o servidor FTP, uma nova sessão TCP é iniciada. Com a conclusão da transferência de dados, a sessão TCP é fechada. Quando a sessão FTP é finalizada, o TCP desempenha ordenadamente um fechamento e um término.

No Wireshark, as informações detalhadas do TCP estão disponíveis no painel de detalhes do pacote (seção do meio). Destaque o primeiro datagrama TCP do computador host e expanda o datagrama TCP. O datagrama TCP expandido é similar ao painel de detalhes de pacote mostrado abaixo.





A imagem acima é um diagrama de um datagrama TCP. Uma explicação de cada campo é fornecida para referência:

* O **TCP Source Port Number** (Número da porta TCP origem) pertence ao host da sessão TCP que abriu uma conexão. O valor é geralmente um valor aleatório acima de 1.023.
* O **TCP Destination Port Number** (Número da porta TCP destino) é usado para identificar o protocolo de camada superior ou aplicação no site remoto. Os valores no intervalo 0-1.023 representam as “portas bem conhecidas” e estão associados a serviços e aplicações populares (conforme descrito na RFC 1700, tais como Telnet, FTP e HTTP). A combinação do endereço IP origem, porta de origem, endereço IP destino e porta de destino identifica de forma exclusiva a sessão para o remetente e o destinatário.

**Observação**: na captura do Wireshark abaixo, a porta de destino é 21, que é FTP. Os servidores FTP ouvem a porta 21 para conexões de clientes FTP.

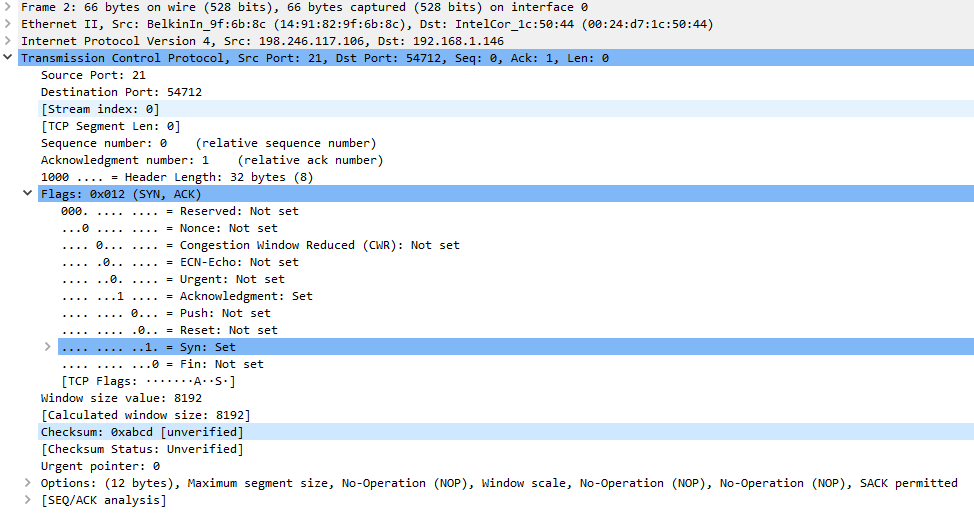
* O **Sequence number** (Número de sequência) especifica o número do último octeto em um segmento.
* O **Acknowledgment number** (Número de confirmação) especifica o próximo octeto esperado pelo destinatário.
* Os **Code bits** (Bits de Código) possuem um significado especial no gerenciamento de sessão e no tratamento de segmentos. Entre valores interessantes estão:
  1. ACK — Confirmação do recebimento de um segmento.
  2. SYN — Sincronizar, ligado somente quando uma nova sessão TCP é negociada durante o handshake triplo do TCP.
  3. FIN — Finalizar, requisição para fechar a sessão TCP.
* O **Window size** (Tamanho da Janela) é o valor da janela deslizante. Ele determina quantos octetos podem ser enviados antes de se esperar por uma confirmação.
* O **Urgent pointer** (Ponteiro de Urgência) só é usado com um flag URG (Urgente) quando o remetente precisa enviar dados urgentes ao destinatário.
* As **Options** (Opções) têm apenas uma opção atualmente e que é o tamanho máximo de segmento TCP (valor opcional).

Usando a captura do Wireshark da primeira inicialização da sessão TCP (bit SYN em 1), preencha as informações sobre o cabeçalho TCP.

Do computador para o servidor do CDC (somente o bit SYN está em 1):

|  |  |
| --- | --- |
| Endereço IP origem | 192.168.0.101 |
| Endereço IP destino | 192.246.117.106 |
| Número da porta de origem | 53462 |
| Número da porta de destino | 21 |
| Número de sequência | 0 |
| Número de confirmação | 0 |
| Tamanho do cabeçalho | 32 |
| Tamanho da janela | 8192 |

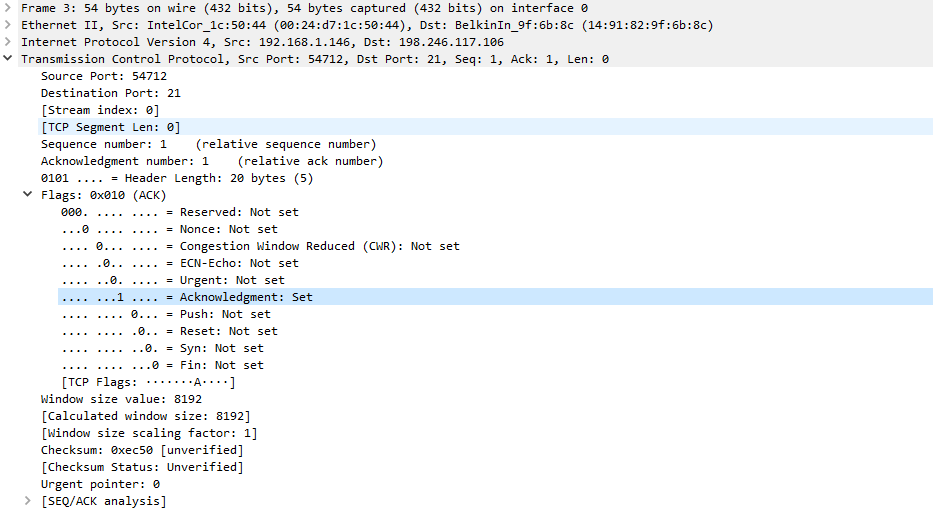
Na segunda captura filtrada do Wireshark, o servidor FTP do CDC confirma a requisição do computador. Observe os valores dos bits SYN e ACK.



Preencha as seguintes informações com relação à mensagem de SYN-ACK.

|  |  |
| --- | --- |
| Endereço IP origem | 198.246.117.106 |
| Endereço IP destino | 192.168.0.101 |
| Número da porta de origem | 21 |
| Número da porta de destino | 53462 |
| Número de sequência | 0 |
| Número de confirmação: | 1 |
| Tamanho do cabeçalho | 32 |
| Tamanho da janela | 8192 |

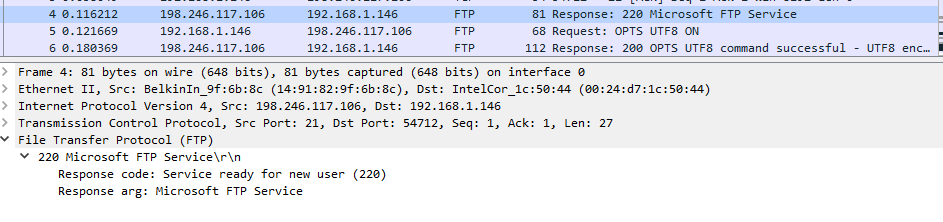
No estágio final da negociação para estabelecer comunicações, o computador envia uma mensagem de confirmação ao servidor. Observe que somente o bit ACK está em 1 e o número de sequência foi incrementado para 1.



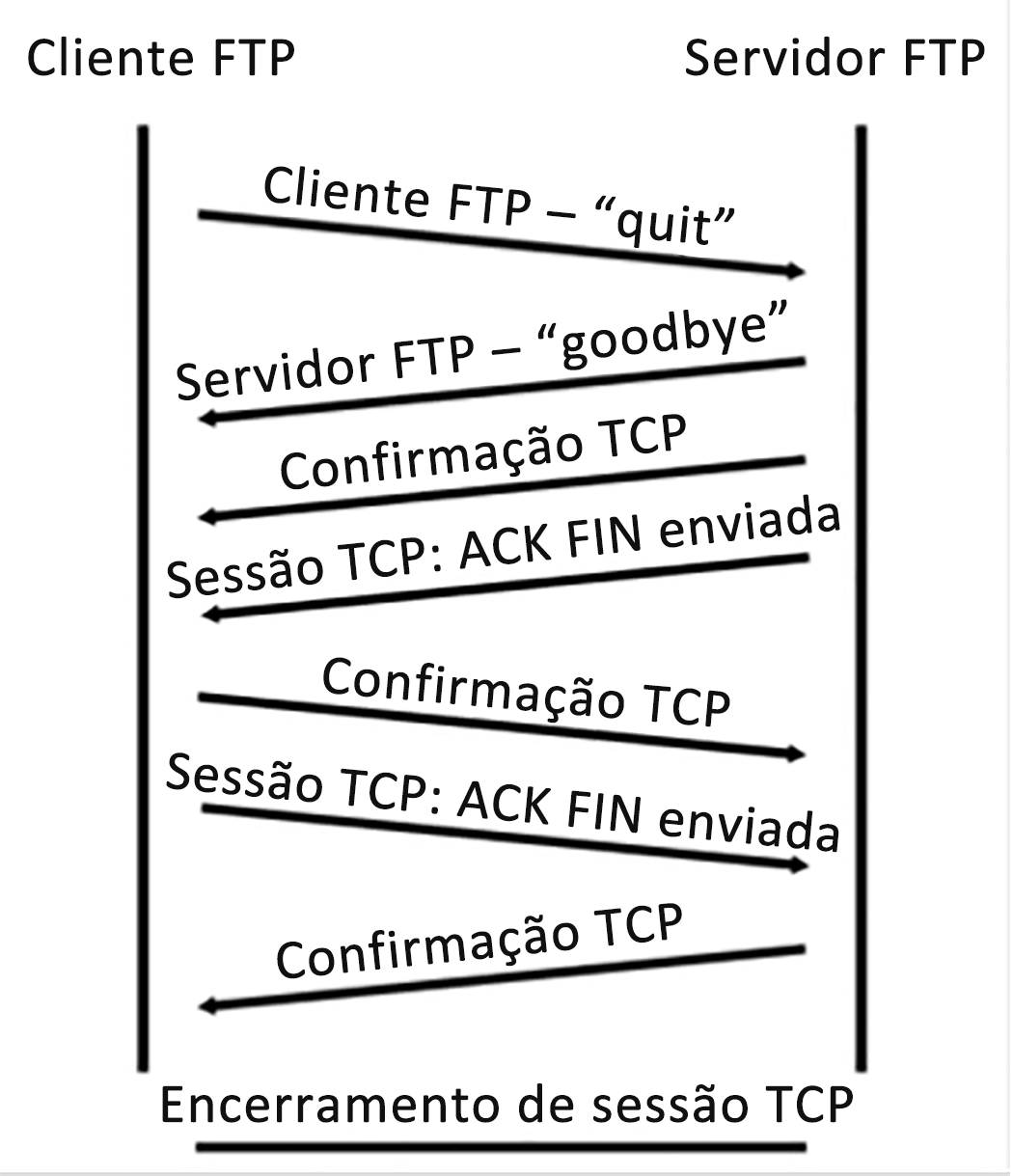
Preencha as seguintes informações com relação à mensagem de ACK.

|  |  |
| --- | --- |
| Endereço IP origem | 192.168.0.101 |
| Endereço IP destino | 198.246.117.106 |
| Número da porta de origem | 53462 |
| Número da porta de destino | 21 |
| Número de sequência | 1 |
| Número de confirmação | 1 |
| Tamanho do cabeçalho | 20 |
| Tamanho da janela | 8192 |

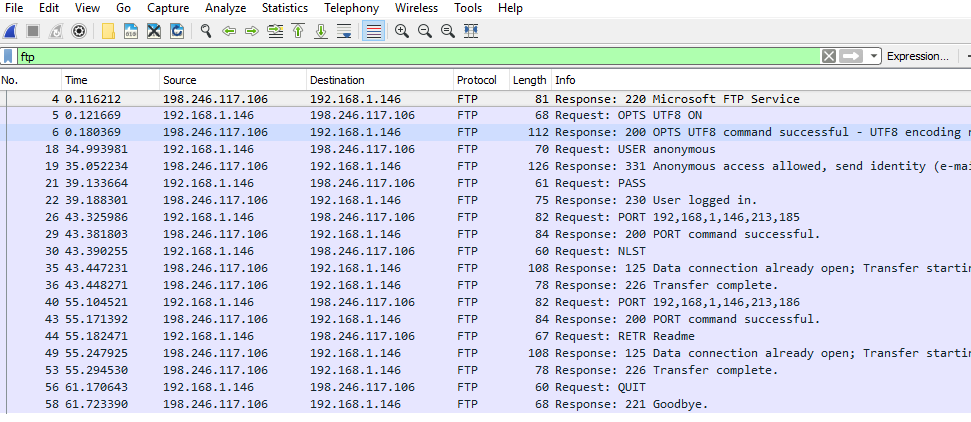
Após uma sessão TCP ser estabelecida, o tráfego FTP pode ocorrer entre o computador e o servidor FTP. O cliente e o servidor FTP se comunicam, sem saber que o TCP possui o controle e o gerenciamento sobre a sessão. Quando o servidor FTP envia uma *Response: 220* ao cliente FTP, a sessão TCP no cliente FTP envia uma confirmação à sessão TCP no servidor. Essa sequência é visível na captura do Wireshark abaixo.



Com a finalização da sessão FTP, o cliente FTP envia um comando “quit”. O servidor FTP confirma o término do FTP com *Response: 221 Goodbye*. Neste momento, a sessão TCP do servidor FTP envia um datagrama TCP ao cliente FTP, anunciando o término da sessão TCP. A sessão TCP do cliente FTP confirma o recebimento do datagrama de término, então, envia seu próprio término da sessão TCP. Quando o originador do término TCP (o servidor FTP) recebe um término duplicado, um datagrama ACK é enviado para confirmar o término e a sessão TCP é fechada. Essa sequência é visível na captura e no diagrama abaixo.



Ao aplicar um filtro ftp, toda a sequência do tráfego FTP pode ser examinada no Wireshark. Observe a sequência dos eventos durante esta sessão FTP. O nome de usuário anonymous foi usado para recuperar o arquivo Readme (Leiame). Quando a transferência for concluída, o usuário terá concluído a sessão FTP.



Aplique o filtro TCP novamente no Wireshark para examinar o término da sessão TCP. Quatro pacotes são transmitidos para o encerramento da sessão TCP. Como a conexão TCP é em full-duplex, cada direção deve ser terminada independentemente. Examine os endereços origem e destino.

Neste exemplo, o servidor FTP não tem mais dados para enviar na transmissão. Ele envia um segmento com o flag FIN definido no quadro 59. O PC envia um ACK para confirmar o recebimento do FIN e encerrar a sessão do servidor para o cliente no quadro 60.

No quadro 61, o computador envia um FIN para o servidor FTP para terminar a sessão TCP. O servidor FTP responde com um ACK para confirmar o FIN do computador no quadro 65. Agora a sessão TCP foi encerrada entre o servidor FTP e o computador.

