Como exportar o certificado TLS da captura de pacote (PCAP) do CUCM

Contents

Introduction

Este documento descreve o procedimento para exportar um certificado de um PCAP do Cisco Unified Communications Manager (CUCM).

Contribuído por Adrian Esquillo, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:
Handshake de TLS (Transport Layer Security)
CUCM Certificate Management
Servidor Secure File Transport Protocol (SFTP)
Real-time Monitoring Tool (RTMT)

Wireshark Application

Componentes Utilizados

CUCM versão 9.X e superior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Uma cadeia de certificado/certificado do servidor pode ser exportada para confirmar se a cadeia de certificado/certificado do servidor fornecida pelo servidor corresponde ao(s) certificado(s) a ser

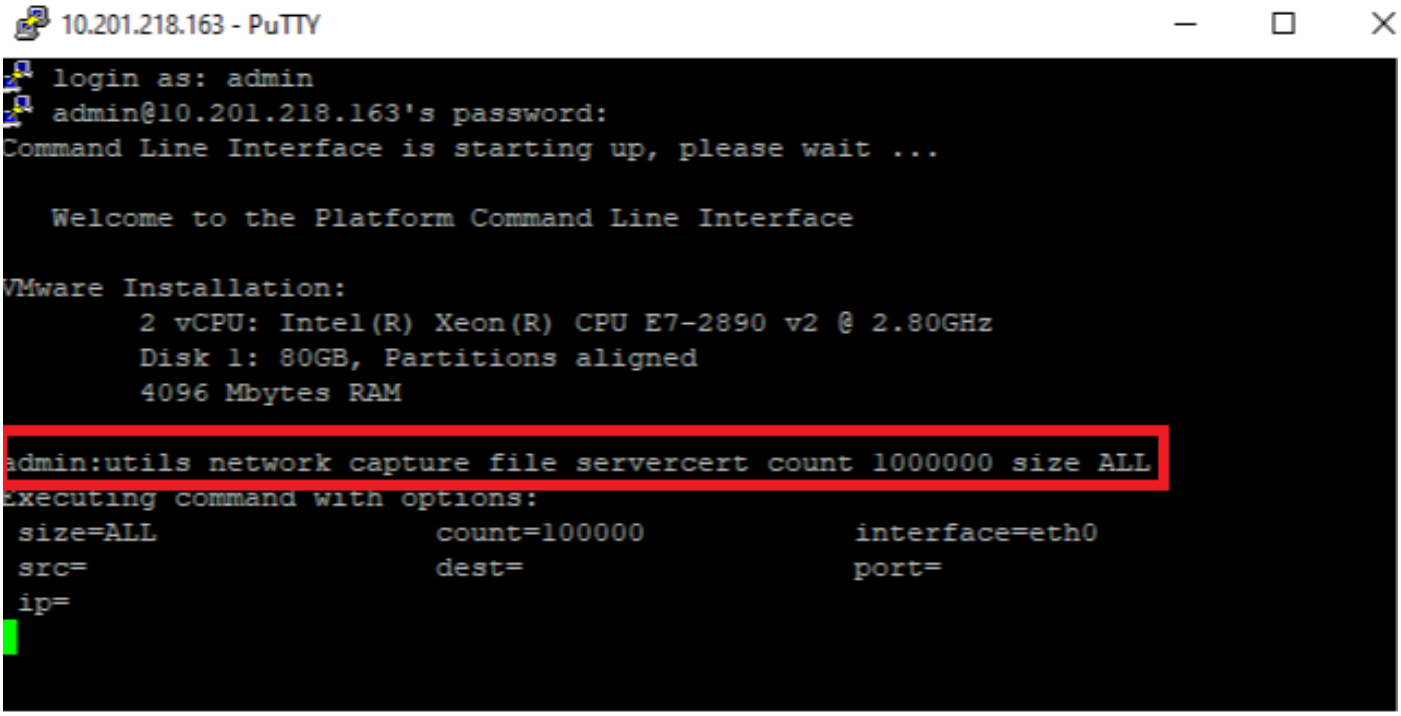
carregado(s) ou que é carregado(s) no CUCM Certificate Management.

Como parte do handshake TLS, o servidor fornece sua cadeia de certificado/certificado do servidor ao CUCM.

Exportar certificado TLS do CUCM PCAP

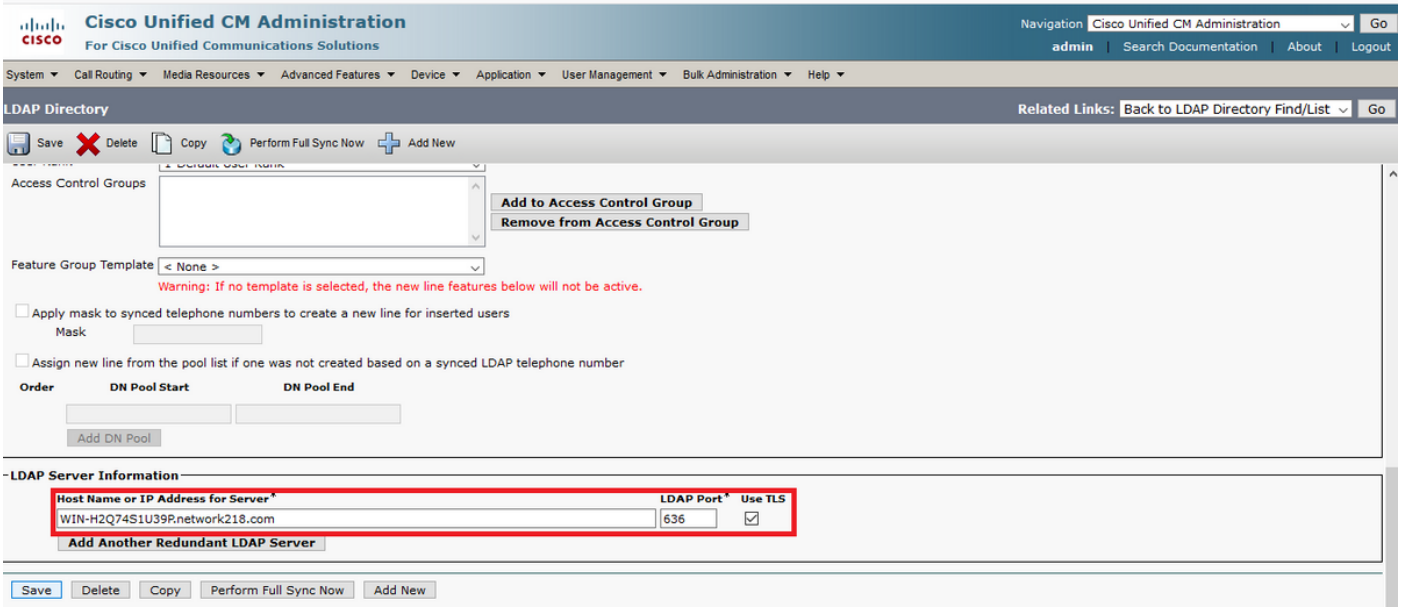
Etapa 1. Iniciar o comando de captura de pacote no CUCM

Estabeleça uma conexão Secure Shell (SSH) com o nó CUCM e execute o comando **utils network capture (ou capture-rotate) file <filename> count 100000 size ALL**, como mostrado na imagem:



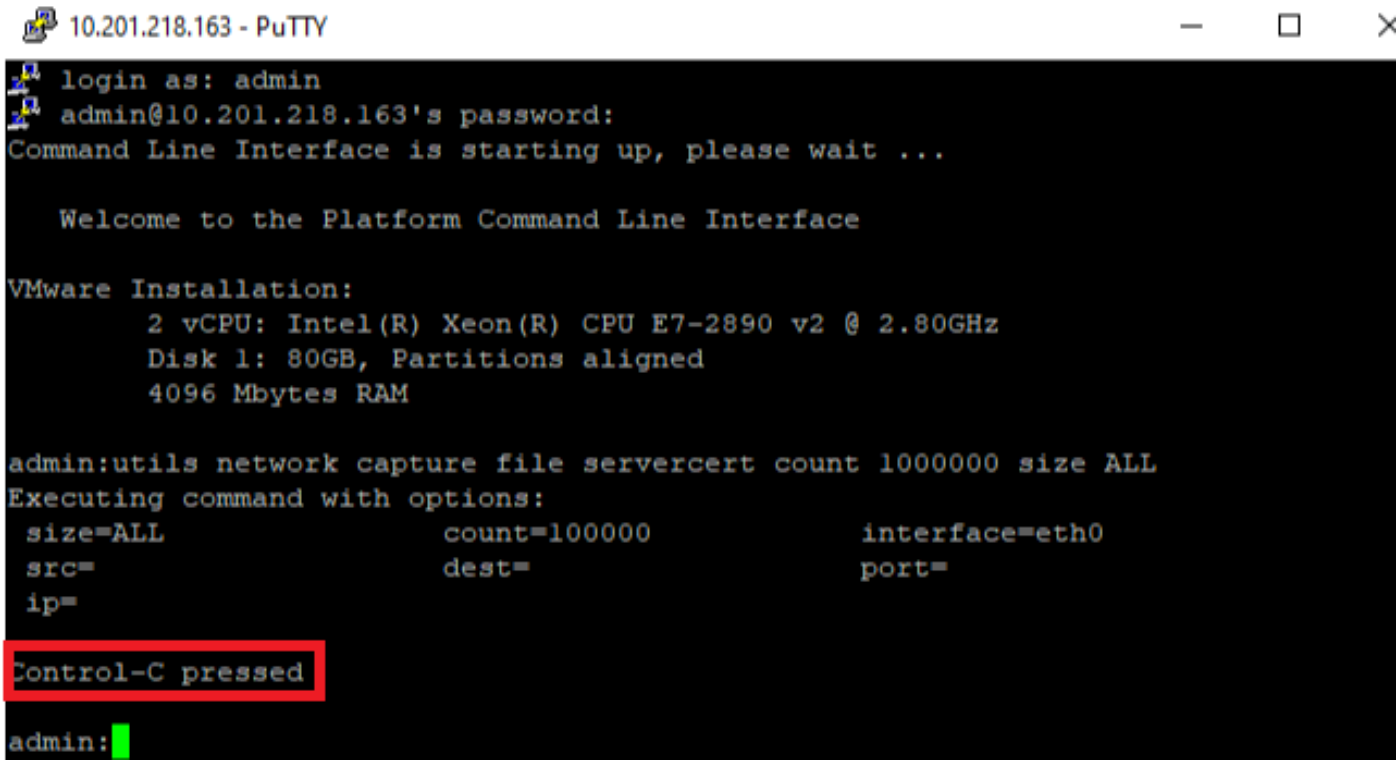
Etapa 2. Iniciar uma conexão TLS entre o servidor e o CUCM

Neste exemplo, você inicia uma conexão TLS entre um servidor Secure Lightweight Diretory Access Protocol (LDAPS) e o CUCM estabelecendo uma conexão na porta TLS 636, como mostrado na imagem:



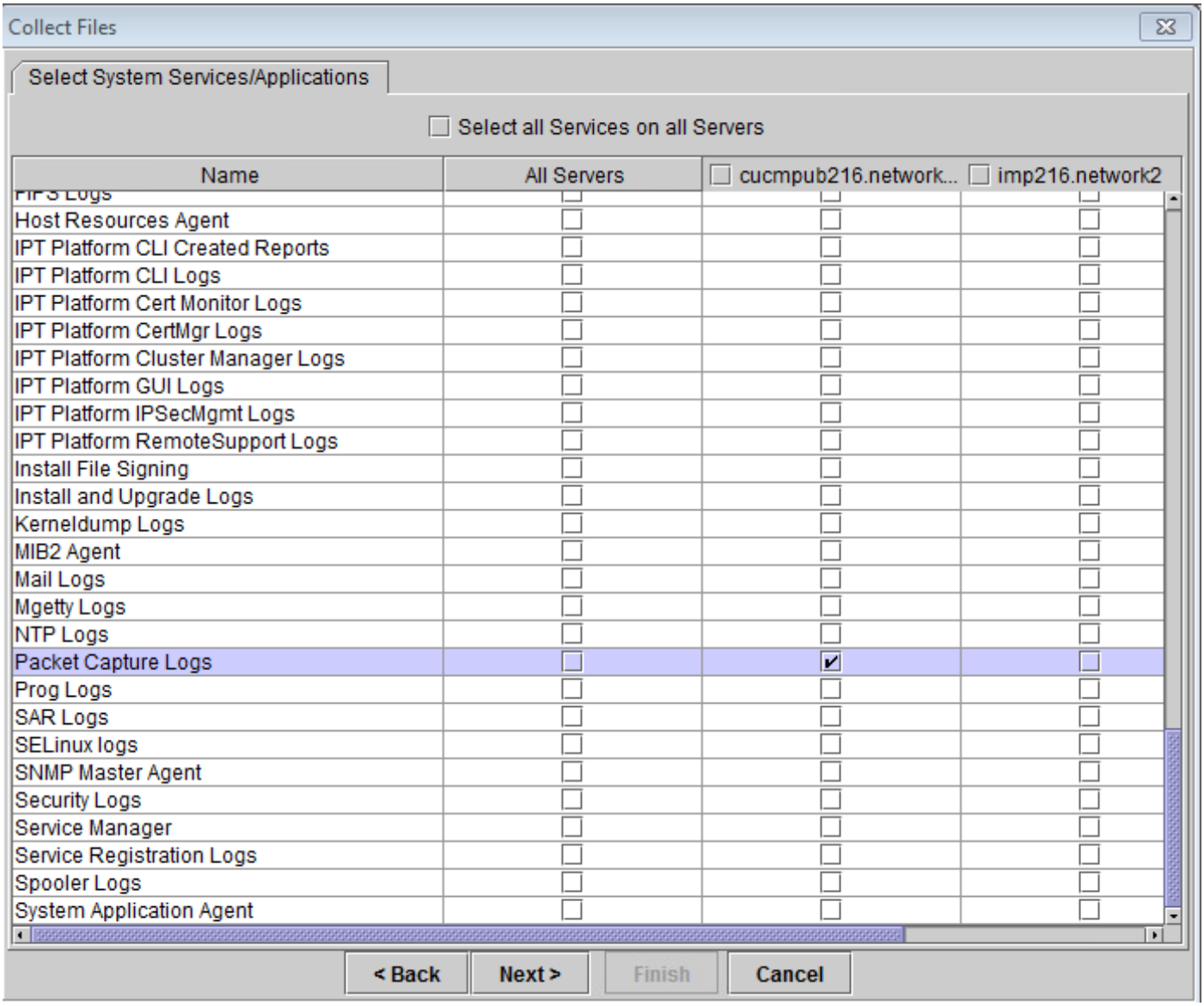
Etapa 3. Parar a PCAP do CUCM após a conclusão do handshake TLS

Pressione **Control-C** para interromper a captura de pacotes, como mostrado na imagem

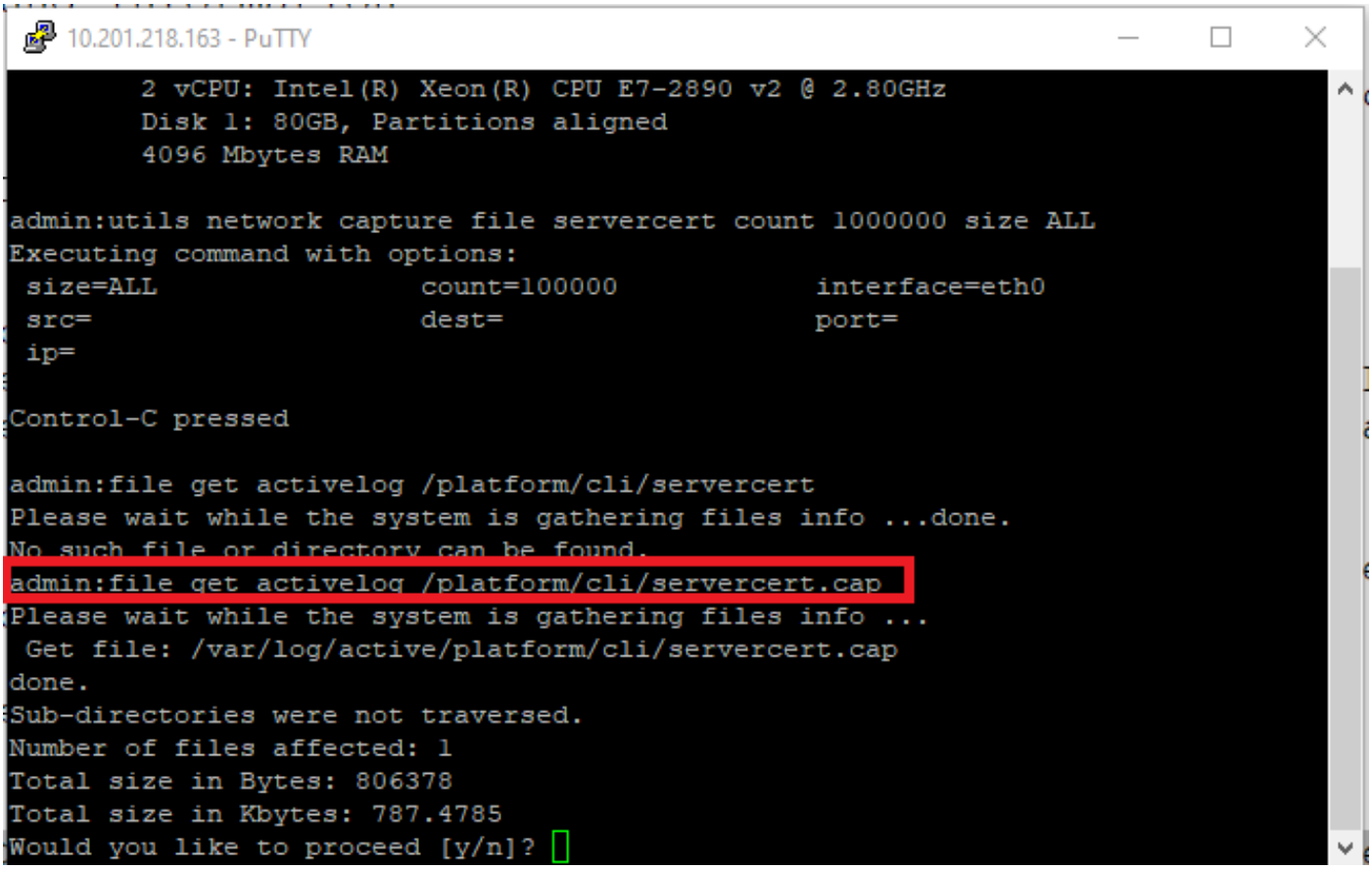


Etapa 4. Baixe o arquivo de captura do pacote por qualquer um dos dois métodos listados

1. Inicie RTMT para o nó CUCM e navegue até **System > Tools > Trace > Trace & Log Central > Collect Files** e marque a caixa **Packet Capture Logs** (continue pelo processo RTMT para fazer o download do pcap), como mostrado na imagem:

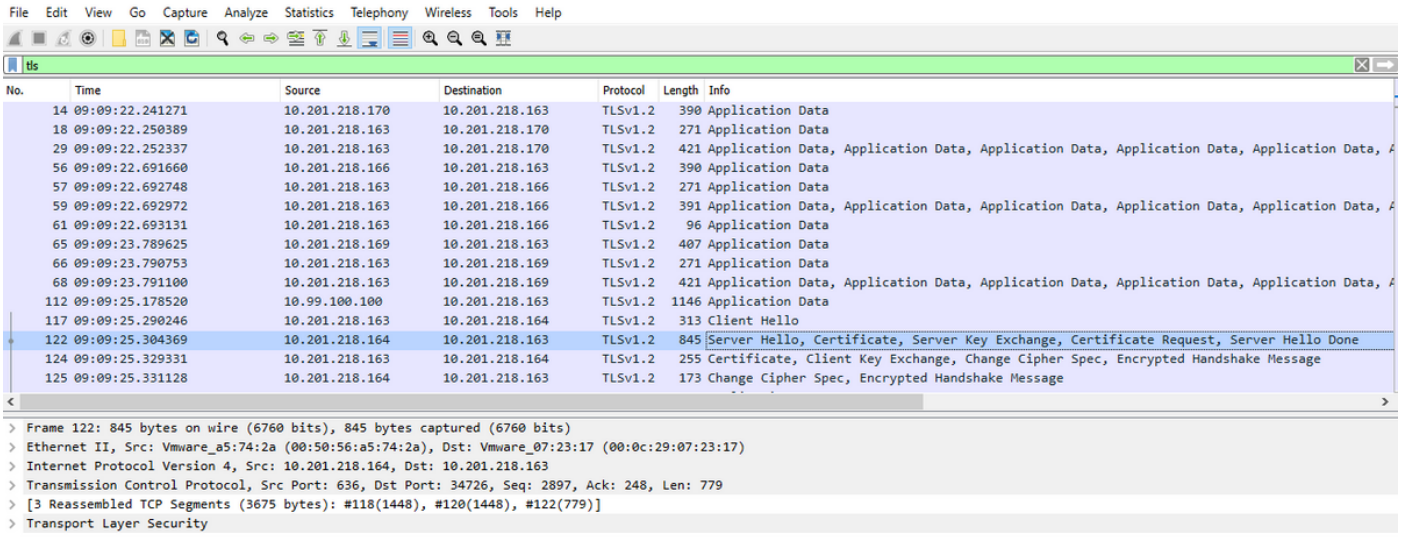


2. Inicie um servidor Secure File Transport Protocol (SFTP) e, na sessão CUCM SSH, execute o **arquivo de** comando **get activelog /patform/cli/<pcap filename>.cap** (continue através dos prompts para baixar o PCAP no servidor SFTP), como mostrado na imagem:

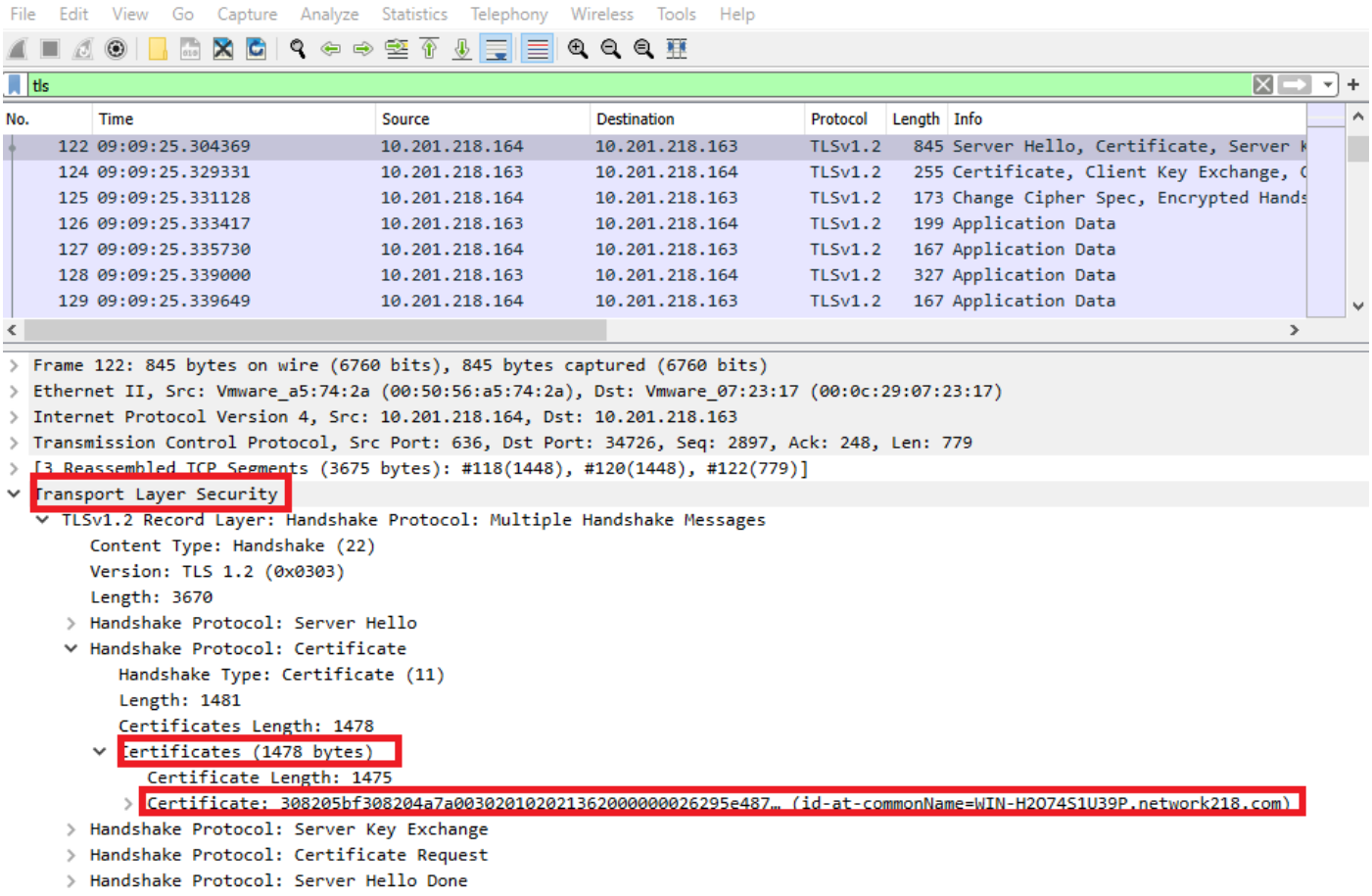


Etapa 5. Determine o número de certificados apresentados ao CUCM pelo servidor

Utilize o aplicativo Wireshark para abrir o pcap e filtrar em **tls** para determinar o pacote com **Servidor Hello** que contém o certificado/cadeia de certificado do servidor apresentado ao CUCM. Este é o quadro 122, como mostrado na imagem:

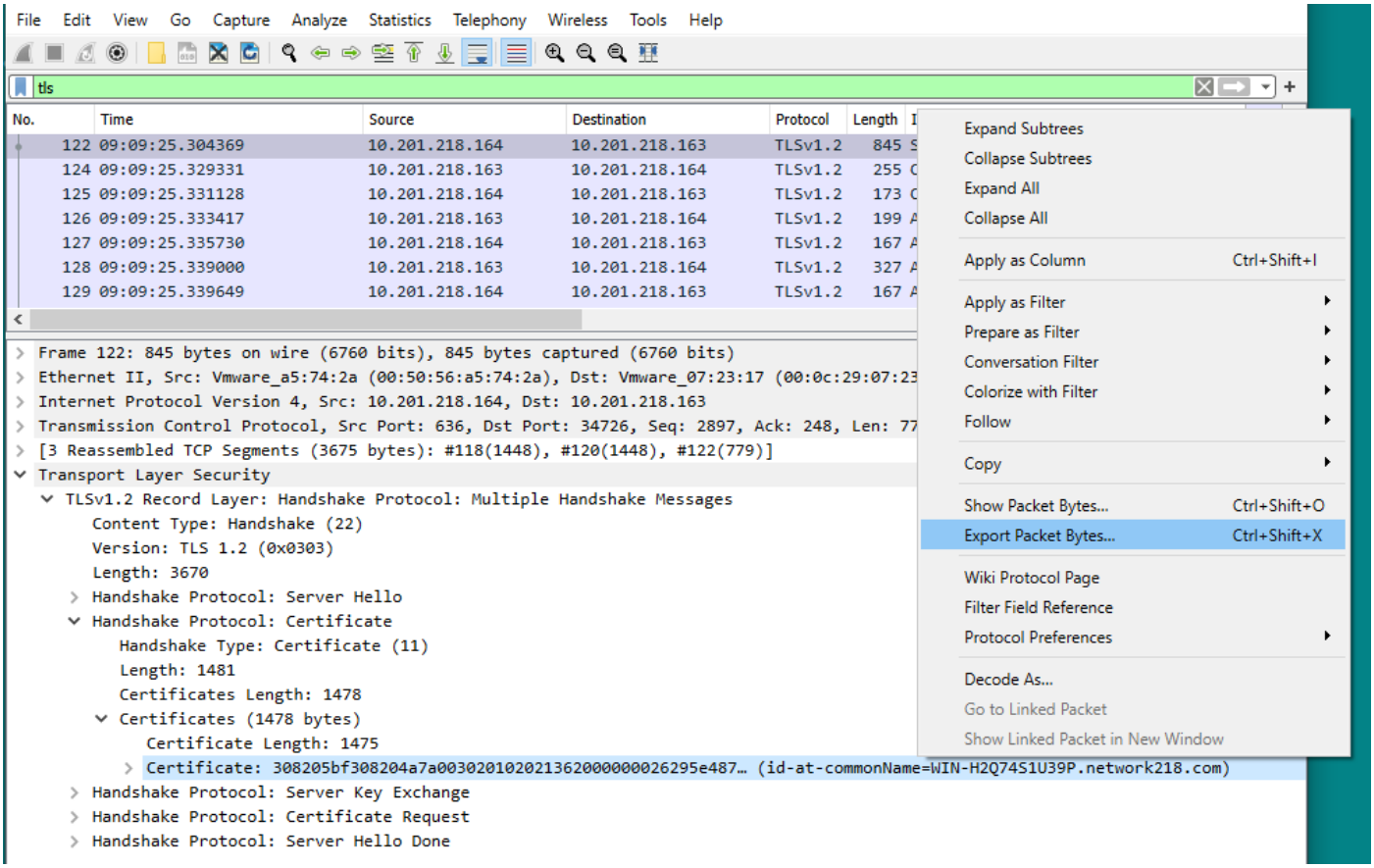


·Expanda as informações **Transport Layer Security > Certificate** do pacote Server Hello com certificado para determinar o número de certificados apresentados ao CUCM. O certificado superior é o certificado do servidor. Nesse caso, apenas 1 certificado, o certificado do servidor, é apresentado como mostrado na imagem:

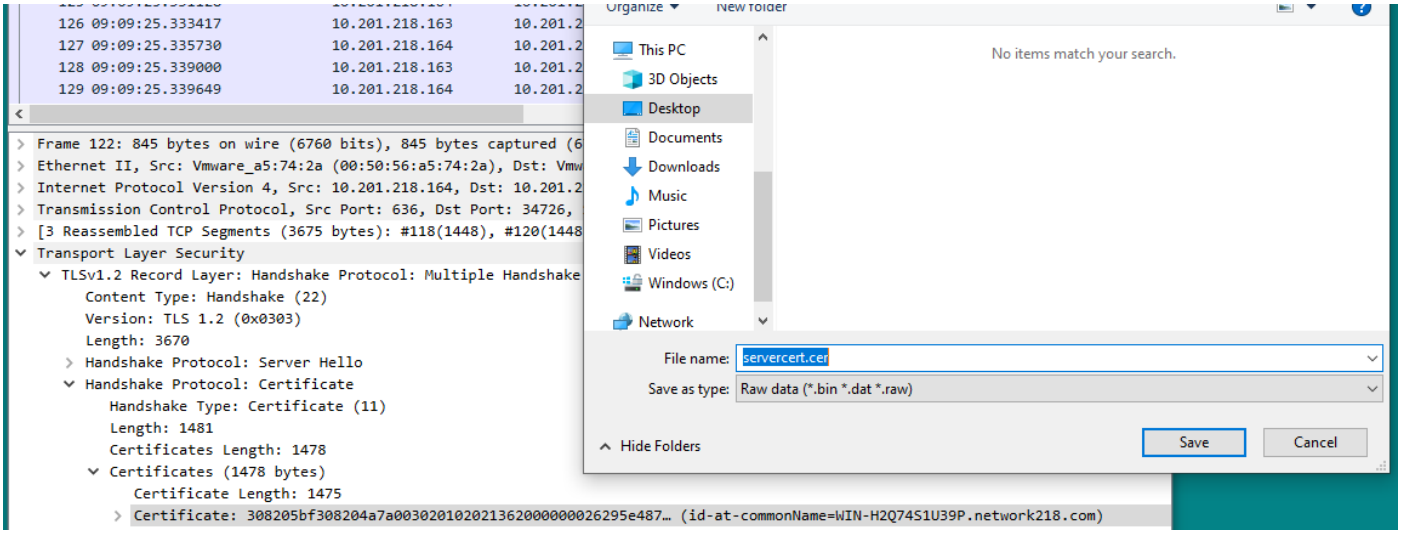


Etapa 6. Exportar a cadeia de certificado/certificado do servidor do CUCM PCAP

Neste exemplo, somente o certificado do servidor é apresentado, portanto é necessário examinar o certificado do servidor. Clique com o botão direito do mouse no certificado do servidor e selecione **Exportar bytes de pacote** para salvar como um certificado .cer, como mostrado na imagem:

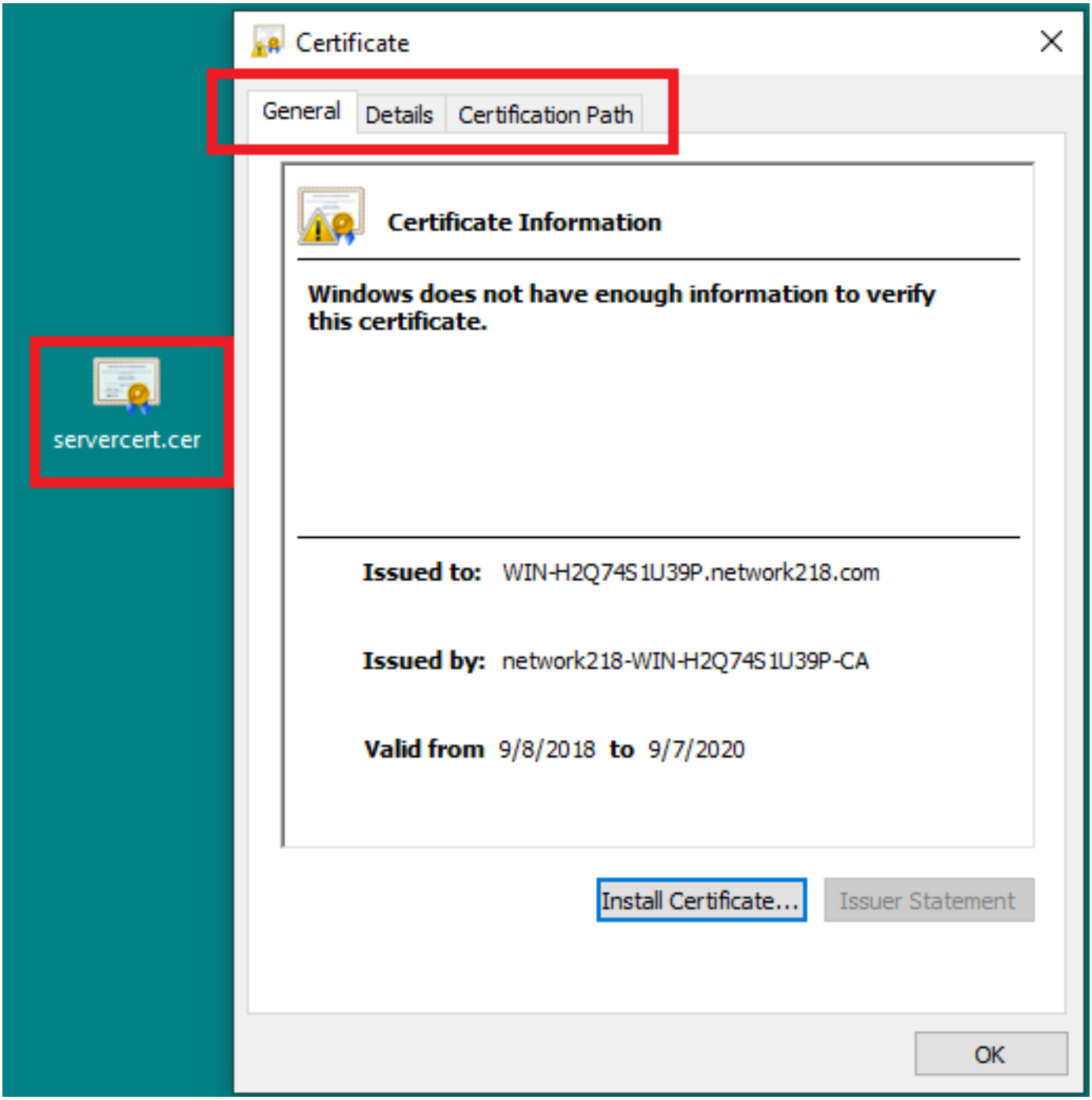


Na janela subsequente, forneça um nome de arquivo .cer e clique em salvar. O arquivo que foi salvo (neste caso, na área de trabalho) foi chamado servercert.cer, como mostrado na imagem:



Passo 7. Abra o arquivo .CER salvo para examinar o conteúdo

Clique duas vezes no arquivo .cer para examinar as informações nas guias **Geral**, **Detalhes** e **Caminho do certificado**, como mostrado na imagem:



Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.