

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Exportar certificado TLS do CUCM PCAP](#)

[Verificar](#)

[Troubleshoot](#)

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

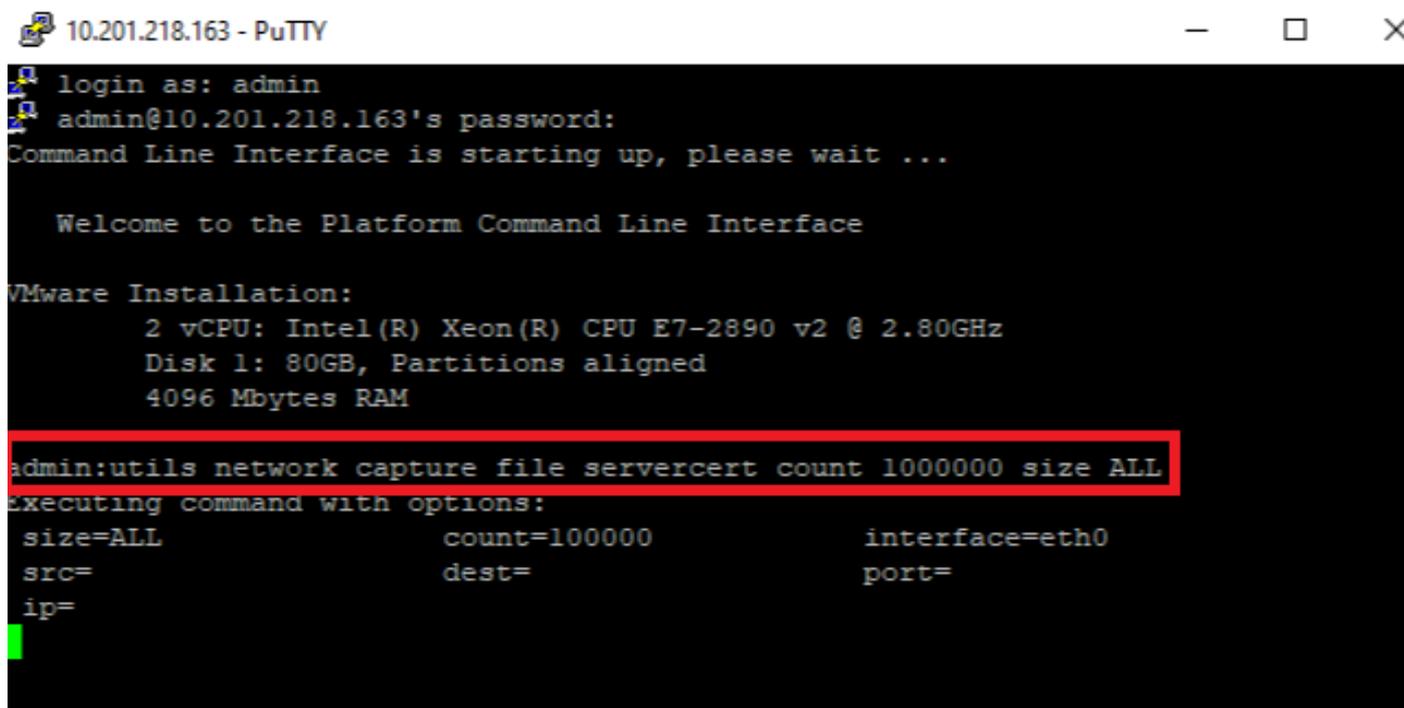
carregado(s) ou que é carregado(s) no CUCM Certificate Management.

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:



```
10.201.218.163 - PuTTY
login as: admin
admin@10.201.218.163's password:
Command Line Interface is starting up, please wait ...

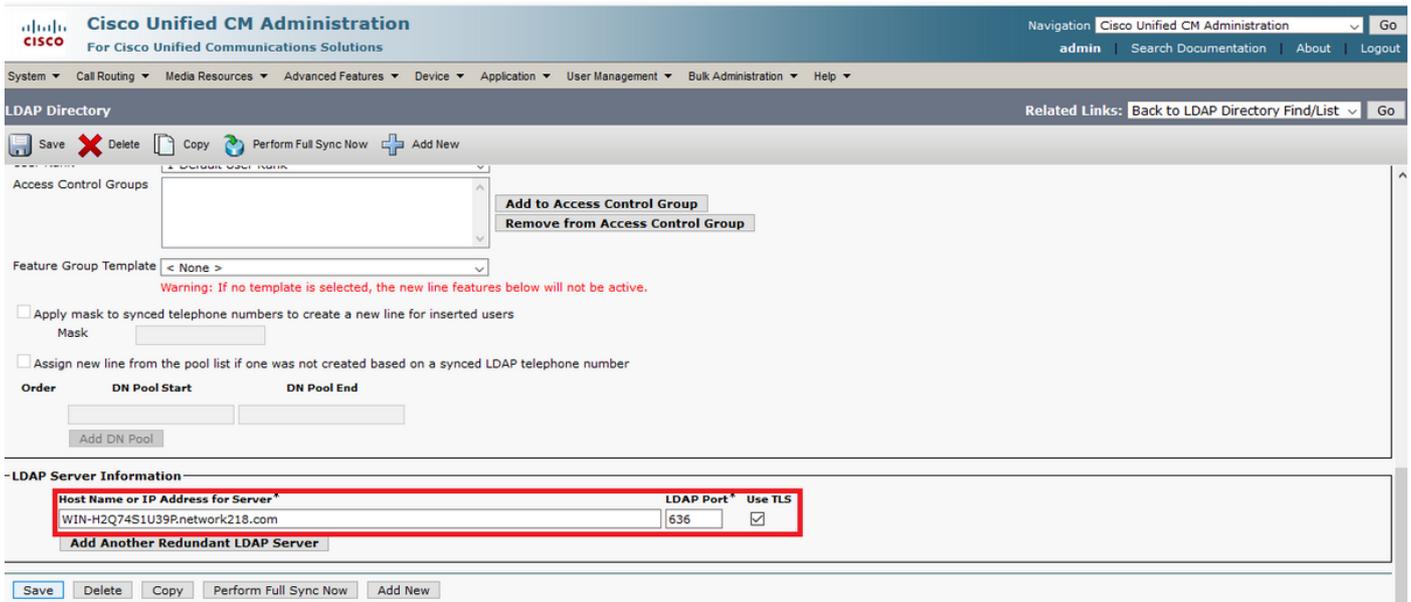
Welcome to the Platform Command Line Interface

VMware Installation:
 2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz
Disk 1: 80GB, Partitions aligned
4096 Mbytes RAM

admin:utils network capture file servercert count 100000 size ALL
executing command with options:
size=ALL          count=100000      interface=eth0
src=              dest=            port=
ip=
```

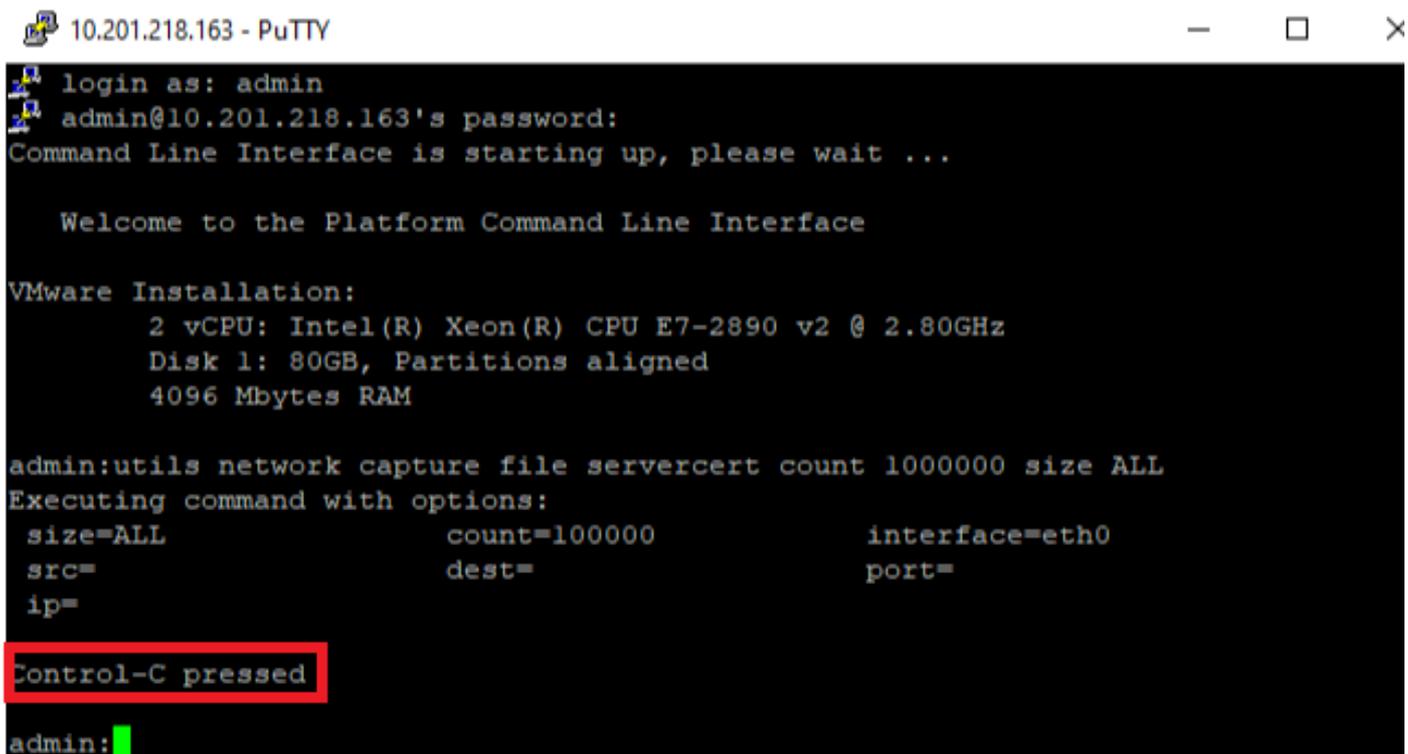
Etapa 2. Iniciar uma conexão TLS entre o servidor e o CUCM

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



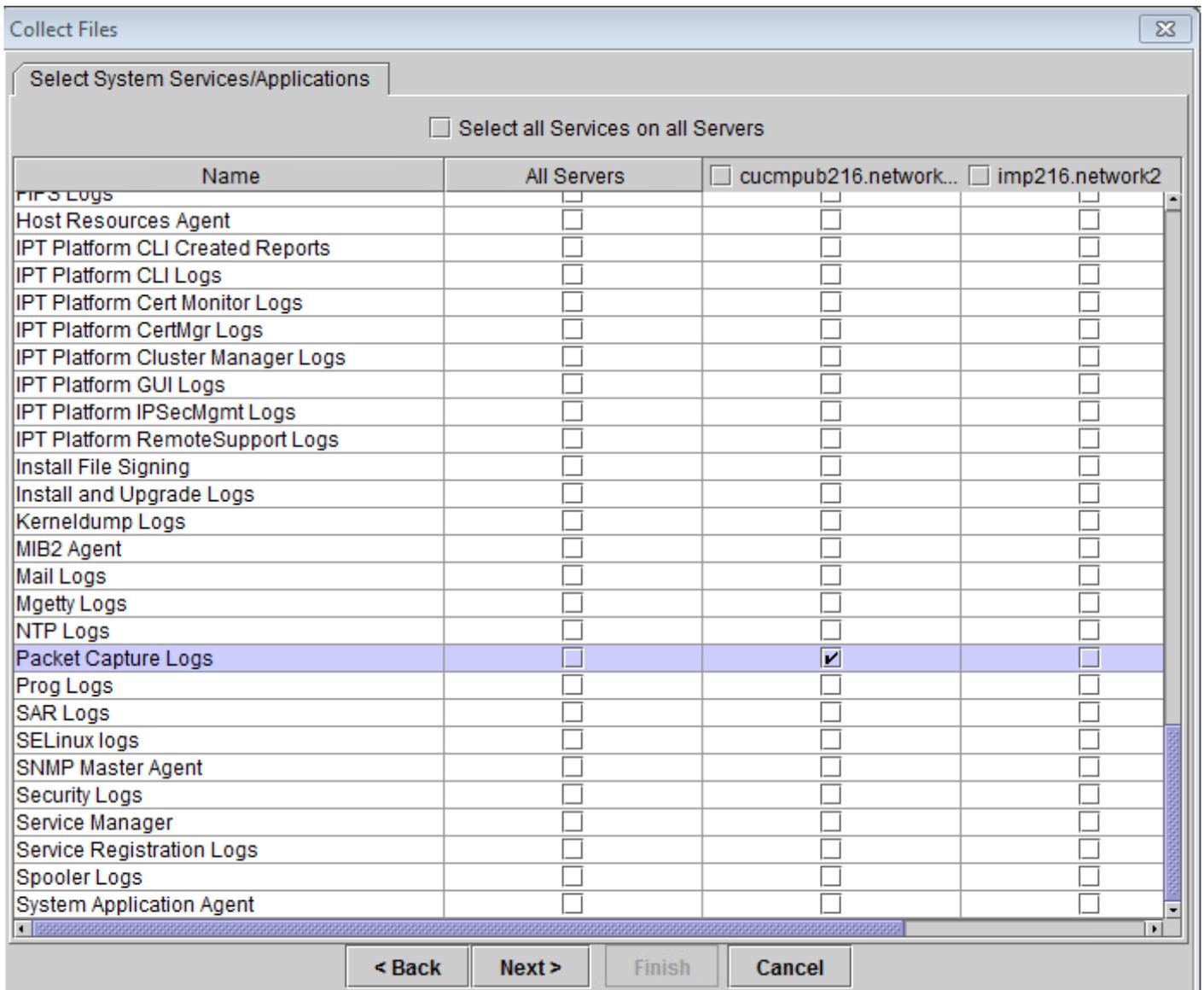
Etapa 3. Parar a PCAP do CUCM após a conclusão do handshake TLS

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 ativelog /patform/cli/<pcap filename>.cap` (continue através dos prompts para baixar o PCAP no servidor SFTP), como mostrado na imagem:

```
10.201.218.163 - PuTTY
2 vCPU: Intel(R) Xeon(R) CPU E7-2890 v2 @ 2.80GHz
Disk 1: 80GB, Partitions aligned
4096 Mbytes RAM

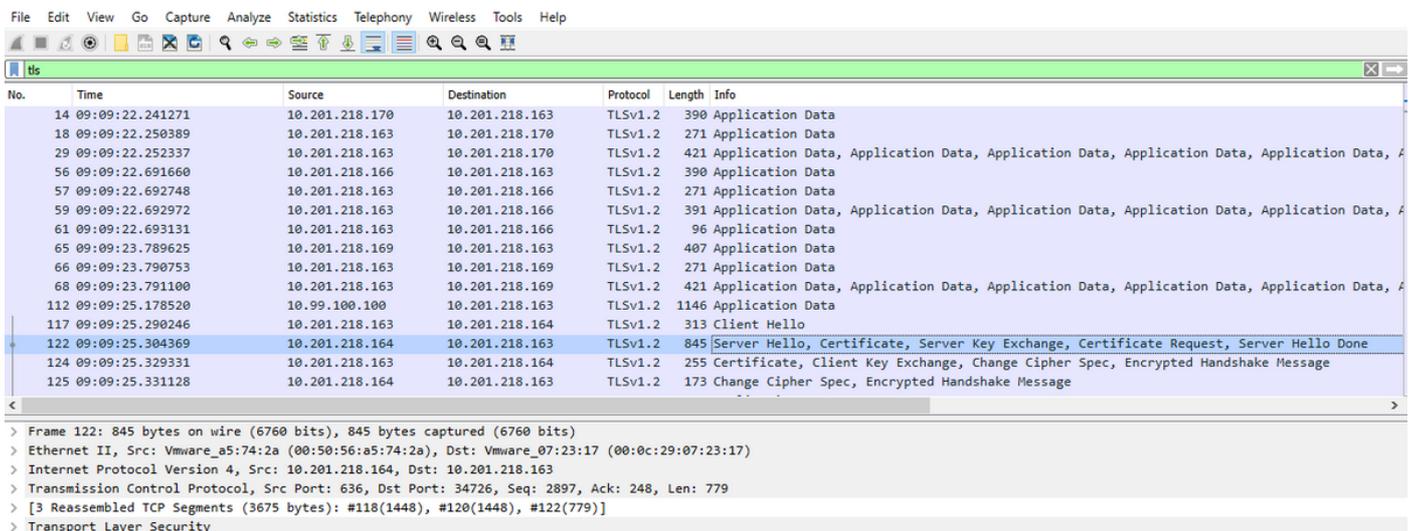
admin:utils network capture file servercert count 1000000 size ALL
Executing command with options:
size=ALL count=100000 interface=eth0
src= dest= port=
ip=

Control-C pressed

admin:file get activelog /platform/cli/servercert
Please wait while the system is gathering files info ...done.
No such file or directory can be found.
admin:file get activelog /platform/cli/servercert.cap
Please wait while the system is gathering files info ...
Get file: /var/log/active/platform/cli/servercert.cap
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 806378
Total size in Kbytes: 787.4785
Would you like to proceed [y/n]? [ ]
```

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:

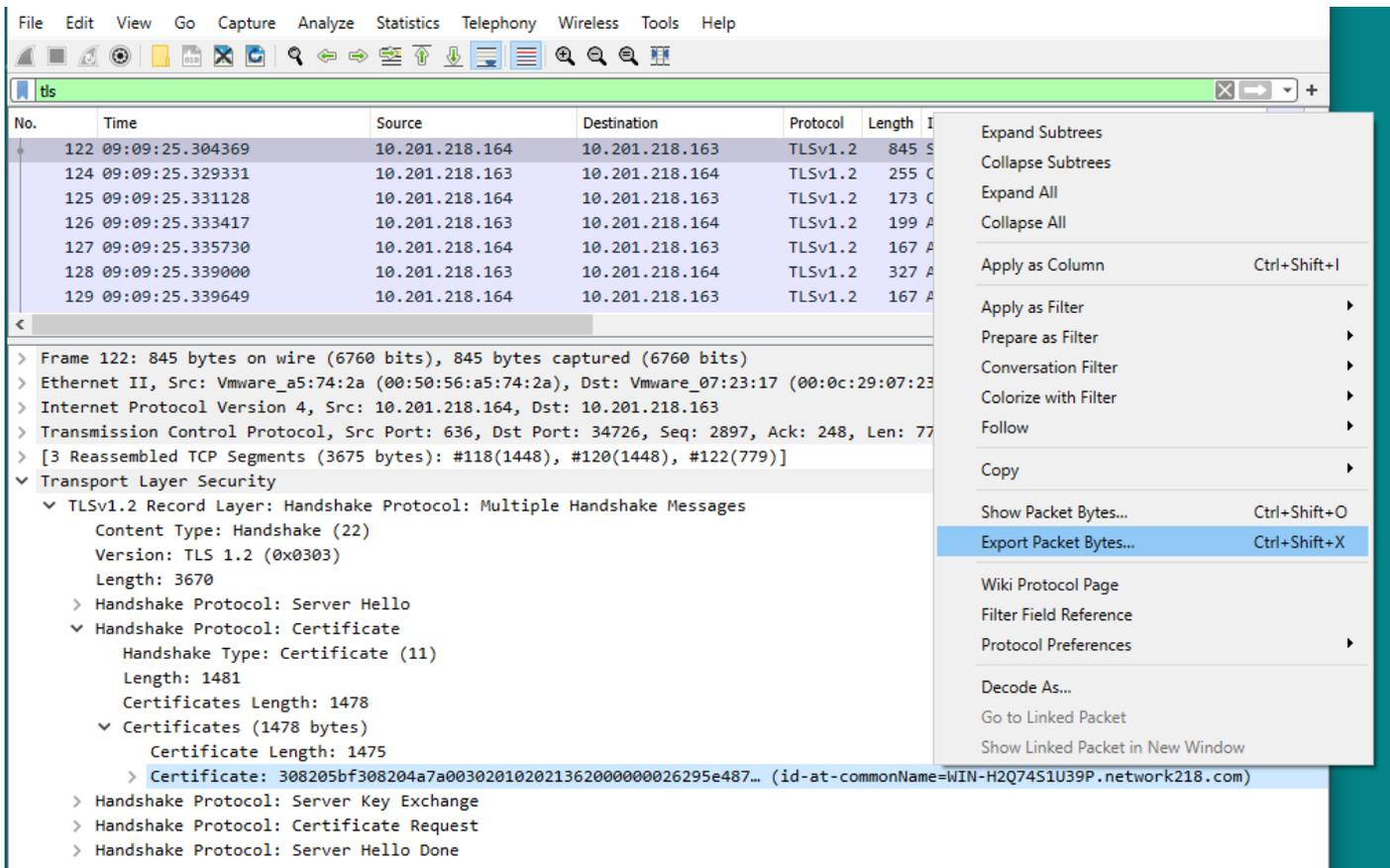
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
122	09:09:25.304369	10.201.218.164	10.201.218.163	TLSv1.2	845	Server Hello, Certificate, Server K
124	09:09:25.329331	10.201.218.163	10.201.218.164	TLSv1.2	255	Certificate, Client Key Exchange, C
125	09:09:25.331128	10.201.218.164	10.201.218.163	TLSv1.2	173	Change Cipher Spec, Encrypted Hands
126	09:09:25.333417	10.201.218.163	10.201.218.164	TLSv1.2	199	Application Data
127	09:09:25.335730	10.201.218.164	10.201.218.163	TLSv1.2	167	Application Data
128	09:09:25.339000	10.201.218.163	10.201.218.164	TLSv1.2	327	Application Data
129	09:09:25.339649	10.201.218.164	10.201.218.163	TLSv1.2	167	Application Data

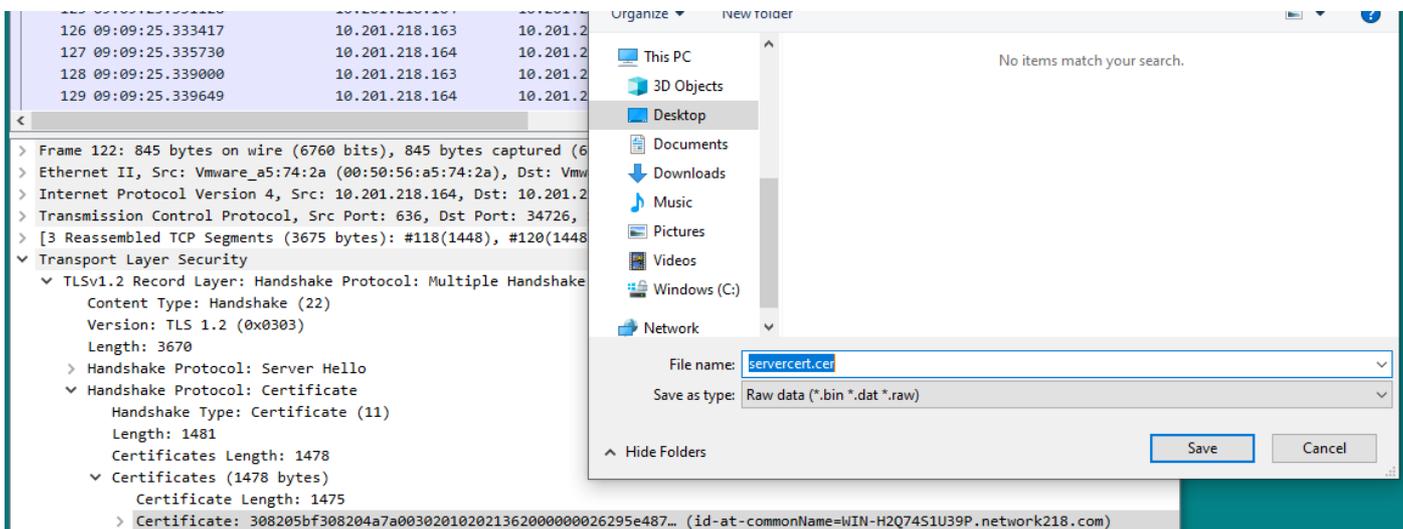
- > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
- > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)
- > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163
- > Transmission Control Protocol, Src Port: 636, Dst Port: 34726, Seq: 2897, Ack: 248, Len: 779
- > [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]
- ✓ **Transport Layer Security**
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3670
 - > Handshake Protocol: Server Hello
 - ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1481
 - Certificates Length: 1478
 - ▼ **Certificates (1478 bytes)**
 - Certificate Length: 1475
 - > **Certificate: 308205bf308204a7a00302010202136200000026295e487... (id-at-commonName=WIN-H207451U39P.network218.com)**
 - > Handshake Protocol: Server Key Exchange
 - > Handshake Protocol: Certificate Request
 - > Handshake Protocol: Server Hello Done

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:

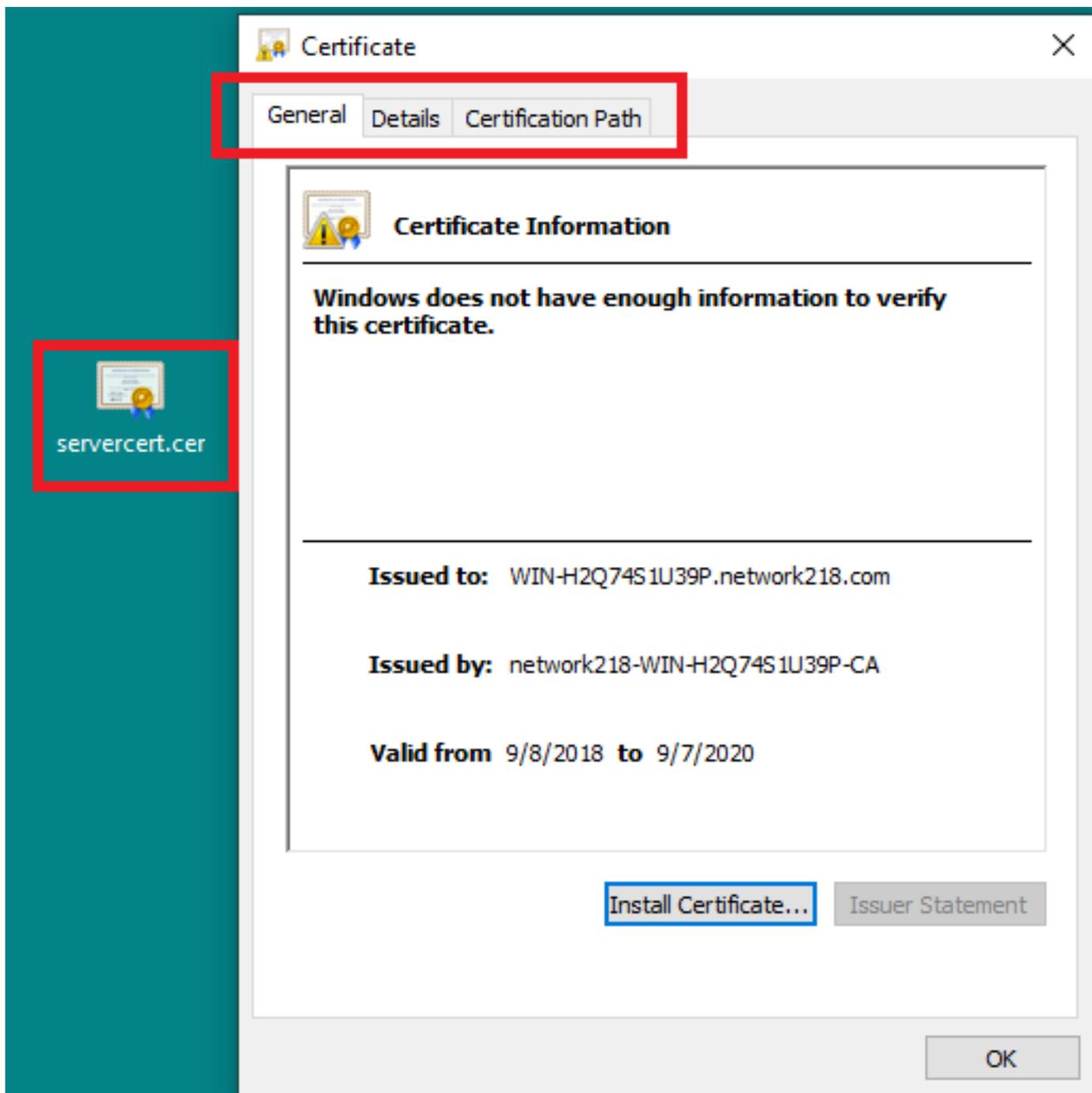


Na janela subsequente, forneça um nome de arquivo .cer e clique em salvar. O arquivo que foi salvo (neste caso, na área de trabalho) foi chamado servercert.cer, como mostrado na imagem:



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.