

Cómo exportar certificados TLS de la captura de paquetes de CUCM (PCAP)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Exportar certificado TLS de CUCM PCAP](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para exportar un certificado desde un PCAP de Cisco Unified Communications Manager (CUCM).

Colaborado por Adrian Esquillo, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Apretón de manos · Transport Layer Security (TLS)

Administración de certificados de CUCM ·

Servidor · Secure File Transport Protocol (SFTP)

Herramienta de supervisión en tiempo real de · (RTMT)

Aplicación · Wireshark

Componentes Utilizados

·CUCM versión 9.X y posterior

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se puede exportar un certificado de servidor/cadena de certificado para confirmar que la cadena de certificado del servidor proporcionada por el servidor coincide con los certificados que se van a

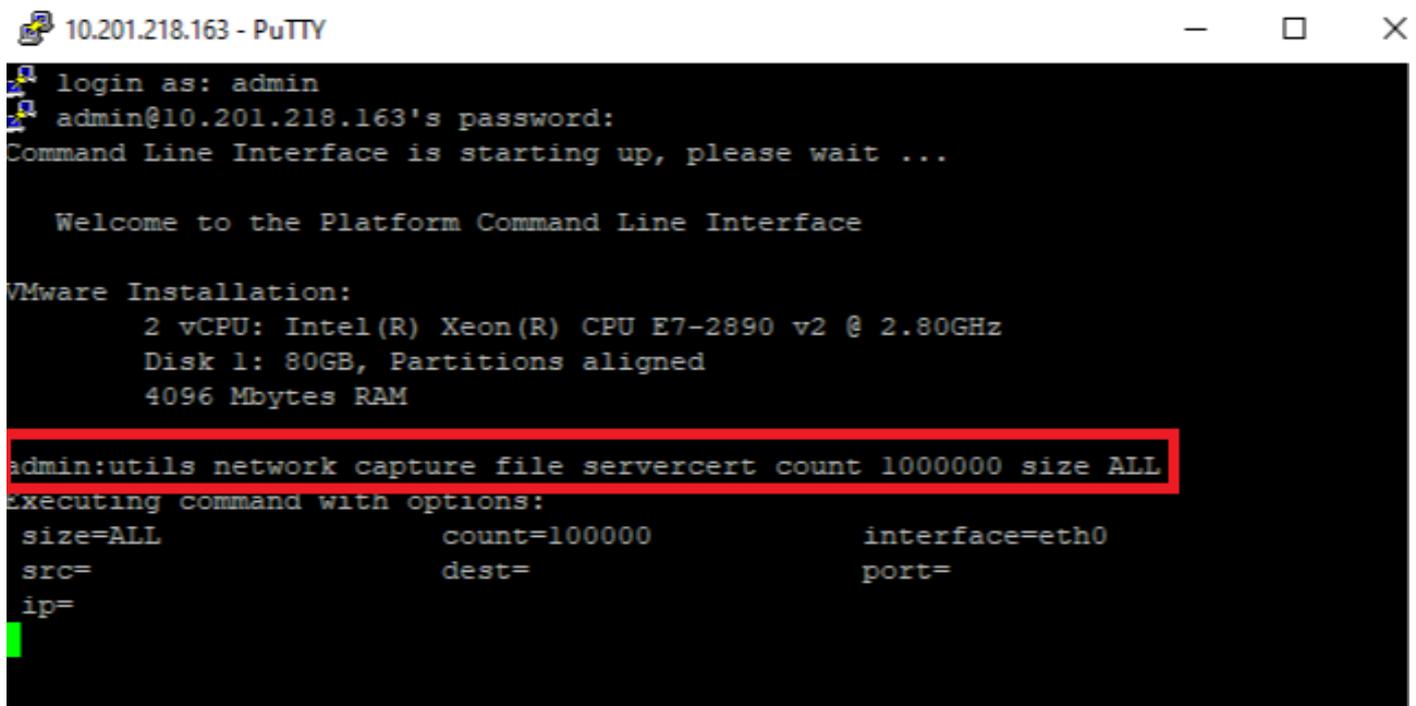
cargar o que se cargan en CUCM Certificate Management.

Como parte del intercambio de señales TLS, el servidor proporciona su cadena de certificado/certificado del servidor a CUCM.

Exportar certificado TLS de CUCM PCAP

Paso 1. Iniciar el comando de captura de paquetes en CUCM

Establezca una conexión Secure Shell (SSH) al nodo CUCM y ejecute el comando **utils network capture (o capture-rotate) file <filename> count 1000000 size ALL**, como se muestra en la imagen:



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

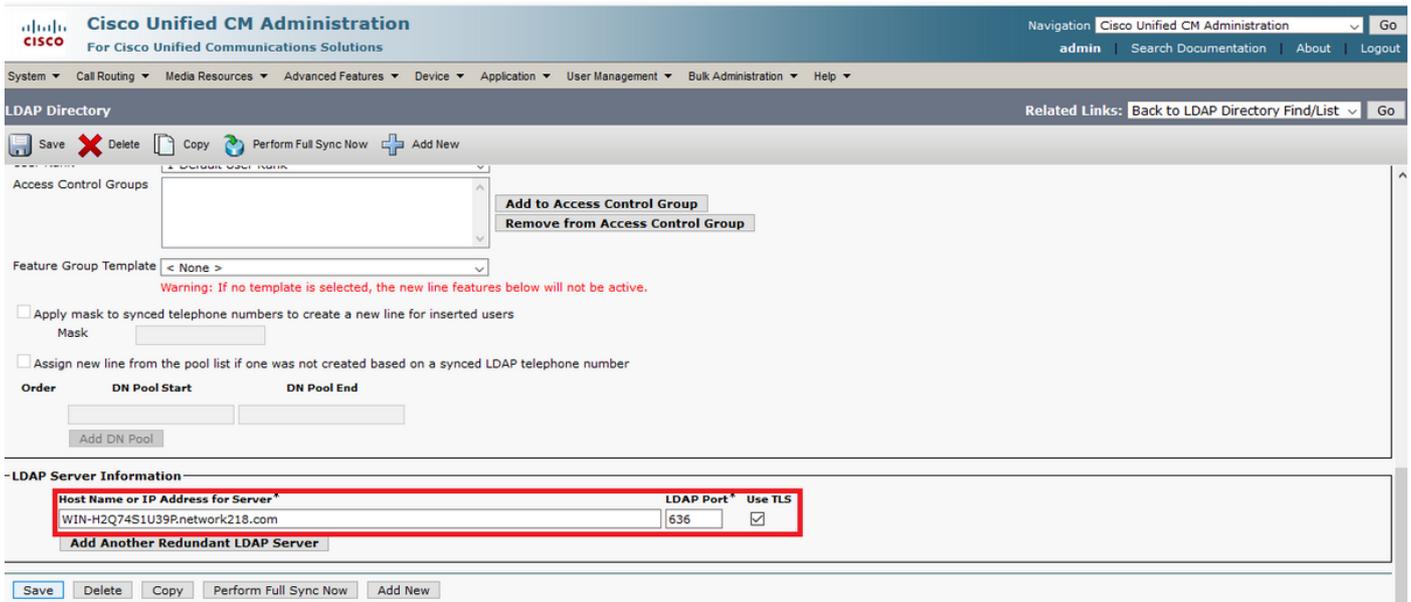
Welcome to the Platform Command Line Interface

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 1000000 size ALL
executing command with options:
size=ALL          count=100000          interface=eth0
src=              dest=                port=
ip=
```

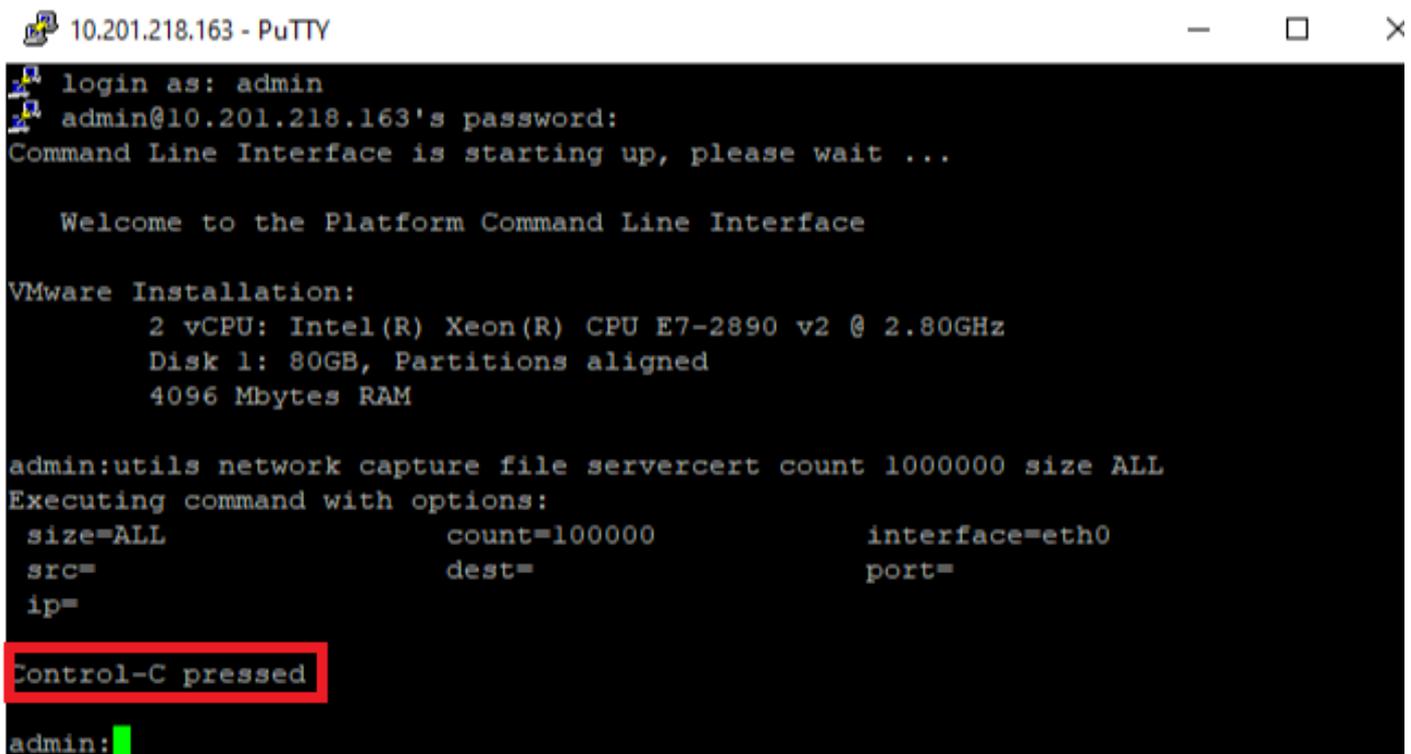
Paso 2. Iniciar una conexión TLS entre el servidor y CUCM

En este ejemplo, se inicia una conexión TLS entre un servidor Secure Lightweight Directory Access Protocol (LDAPS) y CUCM mediante el establecimiento de una conexión en el puerto TLS 636, como se muestra en la imagen:



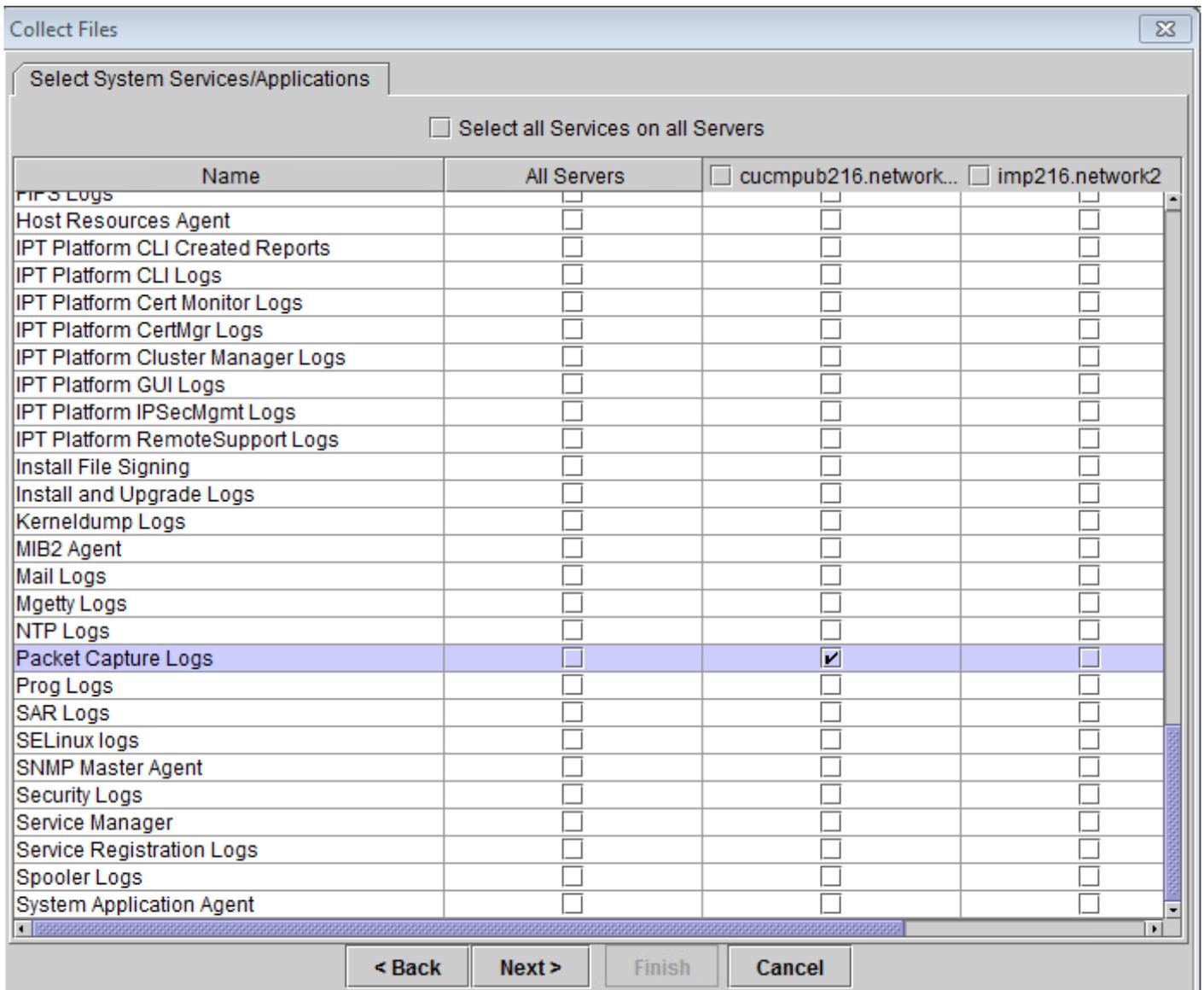
Paso 3. Detener CUCM PCAP después de que se complete el intercambio de señales TLS

Presione **Control-C** para detener la captura de paquetes, como se muestra en la imagen



Paso 4. Descargue el archivo de captura del empaquetador por cualquiera de los dos métodos enumerados

1. Inicie el nodo RTMT para CUCM y navegue hasta **System > Tools > Trace > Trace & Log Central > Collect Files** y marque la casilla **Packet Capture Logs** (continúe con el proceso RTMT para descargar el pcap), como se muestra en la imagen:



2. Inicie un servidor de protocolo seguro de transporte de archivos (SFTP) y en la sesión de CUCM SSH ejecute el comando `file get activelog /platform/cli/<pcap filename>.cap` (siga con las indicaciones para descargar el PCAP en el servidor SFTP), como se muestra en la imagen:

```
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

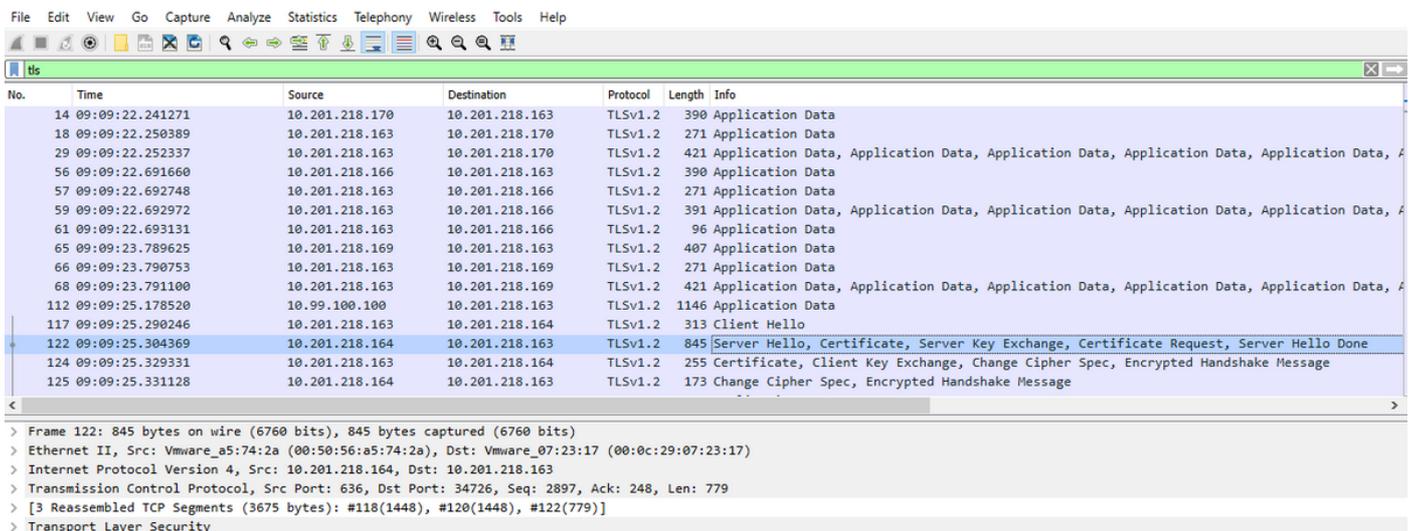
admin:utils network capture file servercert count 1000000 size ALL
Executing command with options:
size=ALL count=100000 interface=eth0
src= dest= port=
ip=

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]? [ ]
```

Paso 5. Determinar el número de certificados presentados a CUCM por el servidor

Utilice la aplicación Wireshark para abrir el pcap y filtrar en **tls** para determinar el paquete con **Server Hello** que contiene la cadena de certificado/certificado del servidor presentado a CUCM. Esta es la trama 122, como se muestra en la imagen:



·Expandar la información **Transport Layer Security > Certificate** del paquete Hello del servidor con el certificado para determinar el número de certificados presentados a CUCM. El certificado superior es el certificado del servidor. En este caso, sólo se presenta un certificado, el certificado del servidor, como se muestra en la imagen:

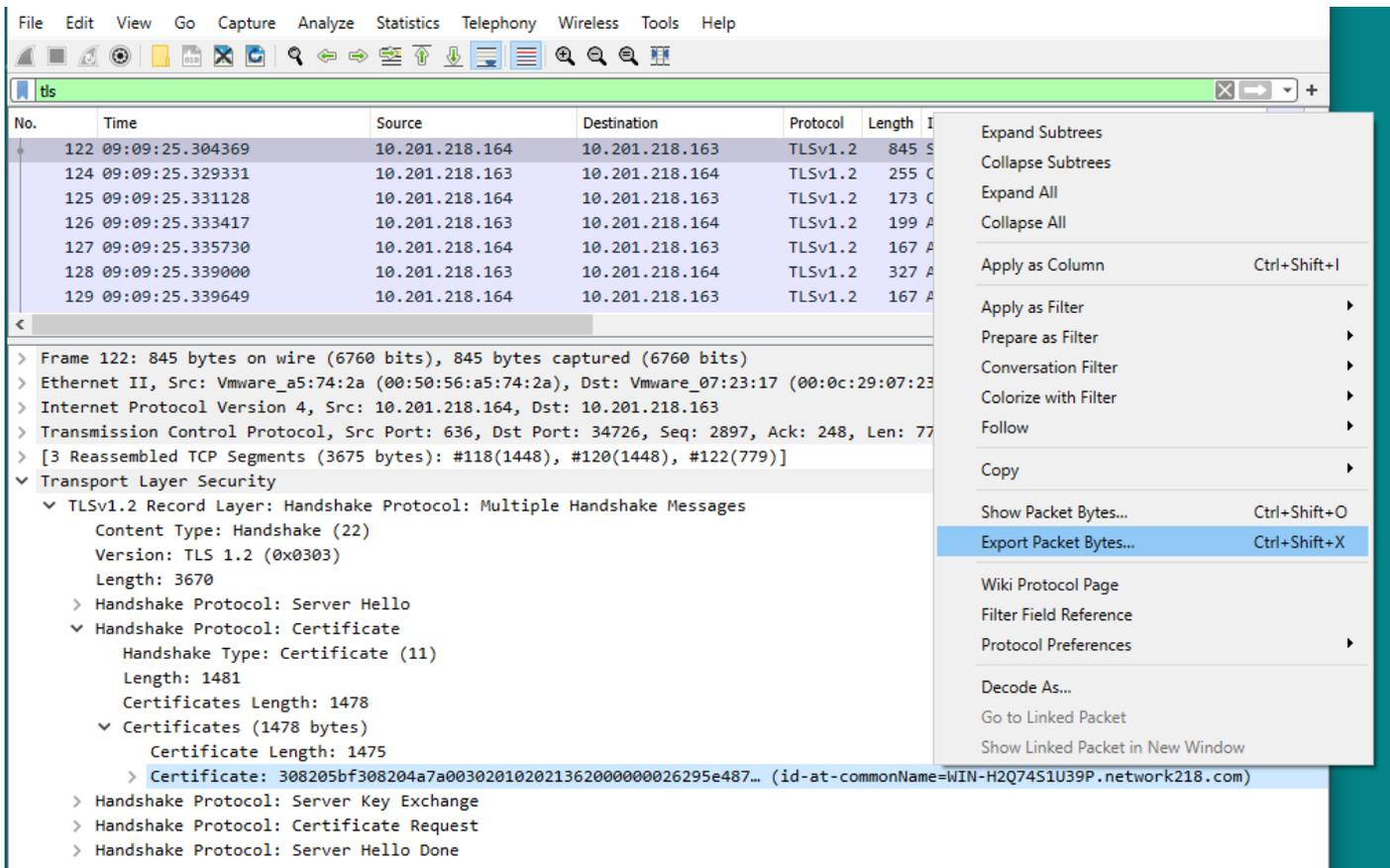
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

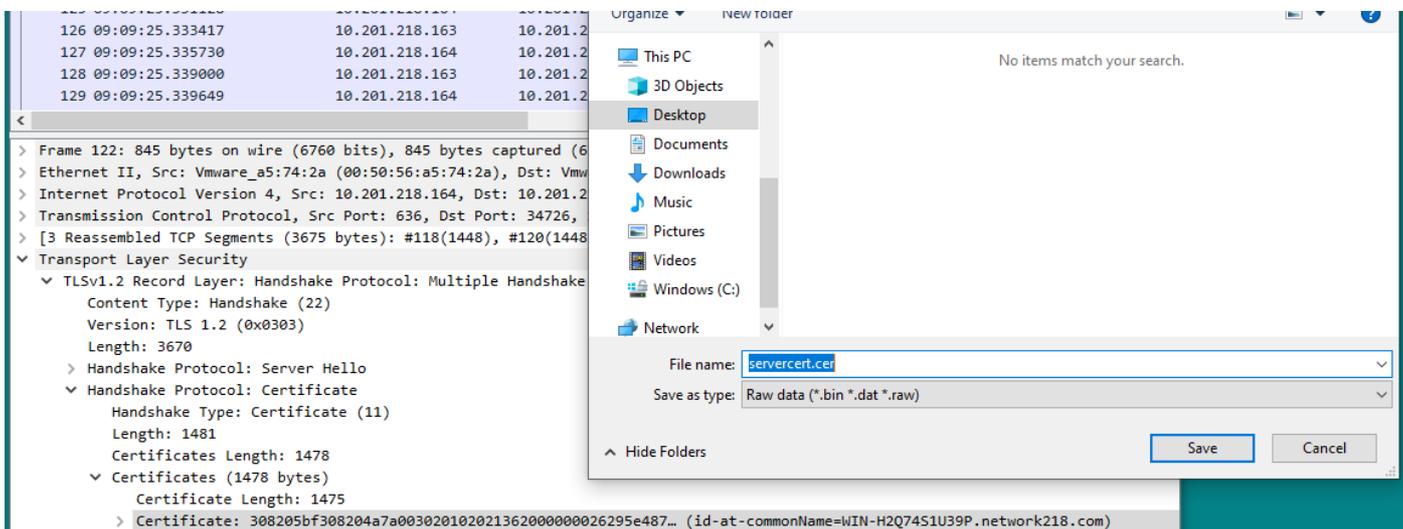
- > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
- > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)
- > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163
- > Transmission Control Protocol, Src Port: 636, 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

Paso 6. Exportar la cadena de certificado/certificado del servidor desde CUCM PCAP

En este ejemplo, sólo se presenta el certificado del servidor, por lo que debe examinar el certificado del servidor. Haga clic con el botón derecho del ratón en el certificado del servidor y seleccione **Exportar bytes de paquete** para guardar como un certificado .cer, como se muestra en la imagen:

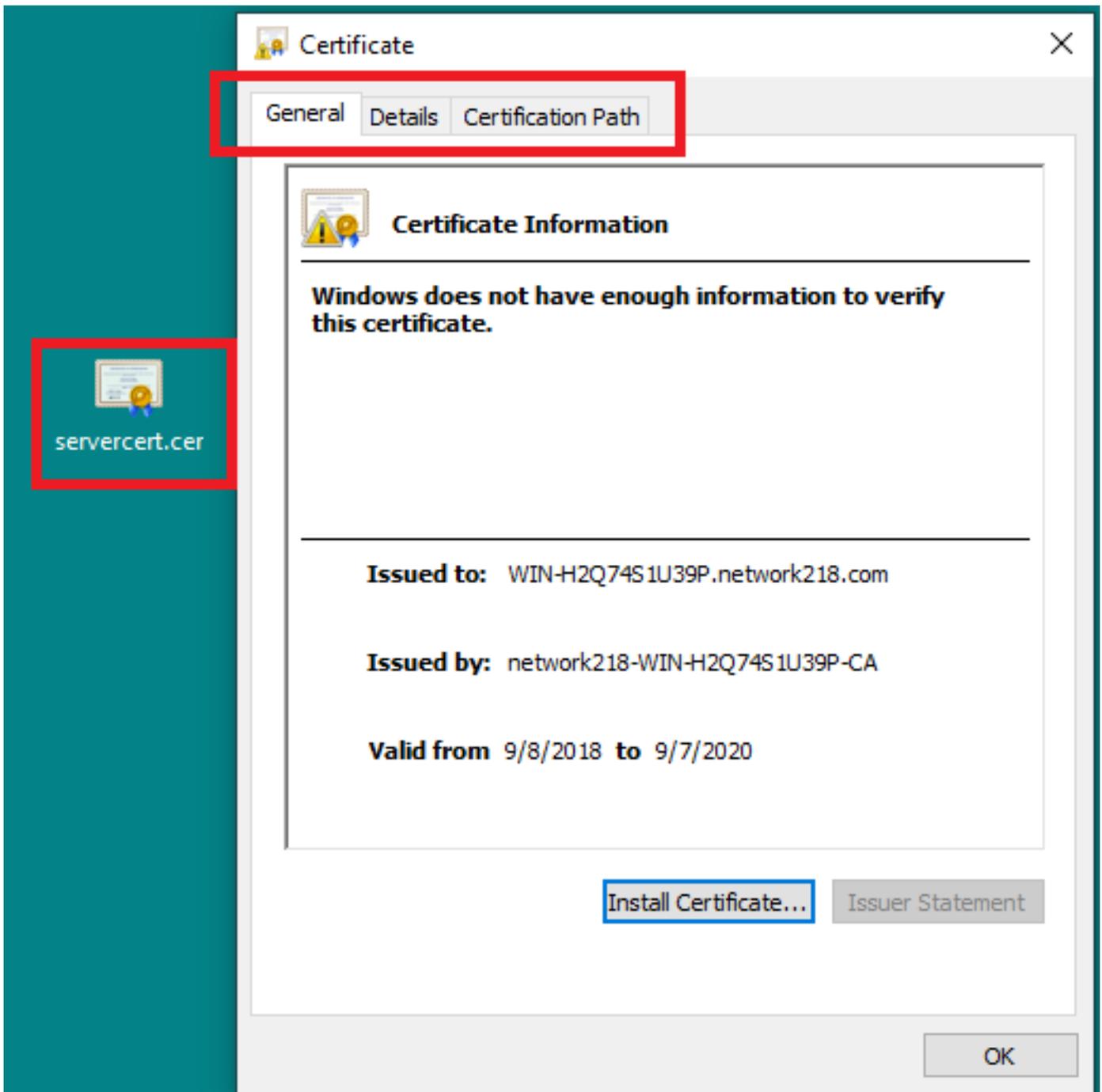


En la ventana siguiente, proporcione un nombre de archivo .cer y, a continuación, haga clic en guardar. El archivo que se guardó (en este caso, en el escritorio) se denominó servercert.cer, como se muestra en la imagen:



Paso 7. Abrir el archivo .CER guardado para examinar el contenido

Haga doble clic en el archivo .cer para examinar la información en las fichas **General**, **Detalles** y **Ruta de certificado**, como se muestra en la imagen:



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.