

Come esportare un certificato TLS da CUCM Packet Capture (PCAP)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esporta certificato TLS da CUCM PCAP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la procedura per esportare un certificato da un protocollo PCAP di Cisco Unified Communications Manager (CUCM).

Contributo di Adrian Esquillo, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Handshake Transport Layer Security (TLS)
- Gestione certificati CUCM
- Server SFTP (Secure File Transport Protocol)
- Strumento di monitoraggio in tempo reale (RTMT)

- Applicazione Wireshark

Componenti usati

- CUCM release 9.X e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

È possibile esportare un certificato server/catena di certificati per verificare che il certificato

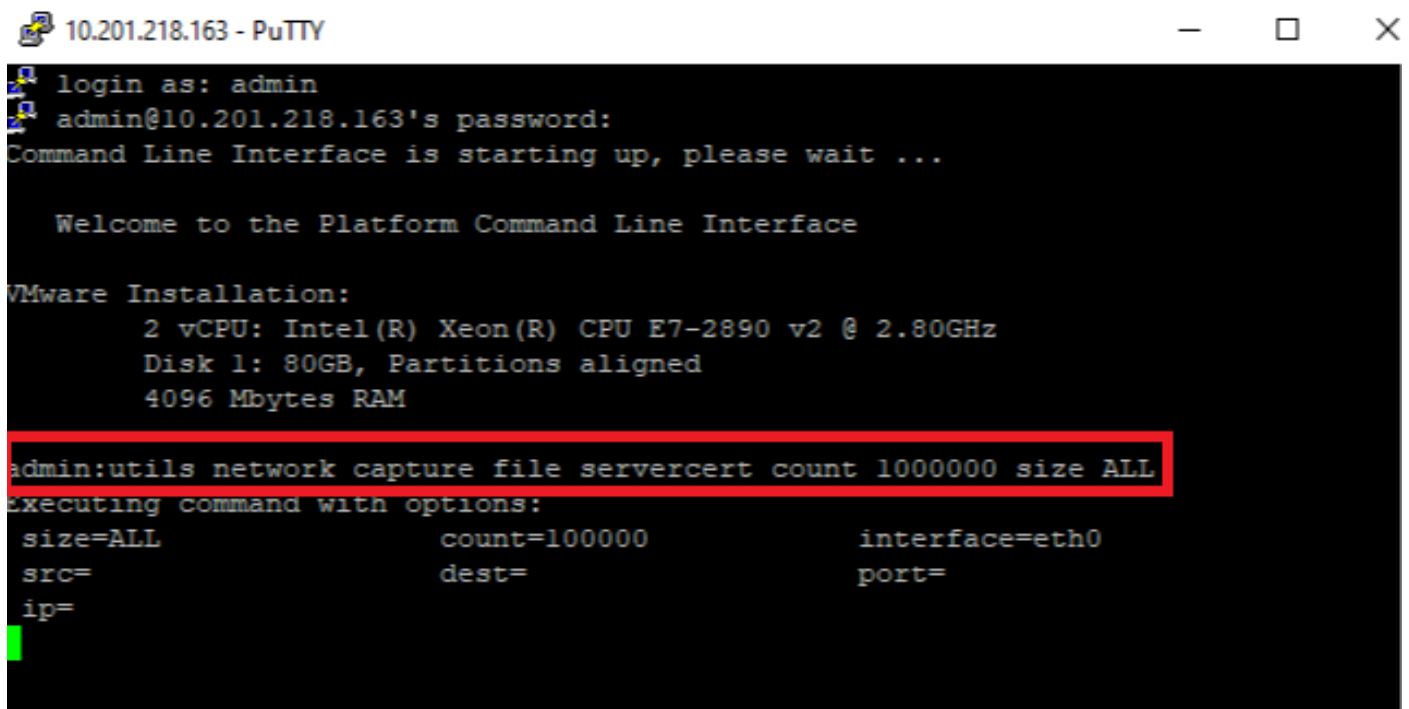
server/catena di certificati forniti dal server corrisponda ai certificati da caricare o caricati in Gestione certificati CUCM.

Come parte dell'handshake TLS, il server fornisce a CUCM il proprio certificato/catena di certificati server.

Esporta certificato TLS da CUCM PCAP

Passaggio 1. Avviare il comando packet capture su CUCM

Stabilire una connessione Secure Shell (SSH) al nodo CUCM ed eseguire il comando **utilizza network capture (o capture-rotate) file <nomefile> count 1000000 size ALL**, come mostrato nell'immagine:



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

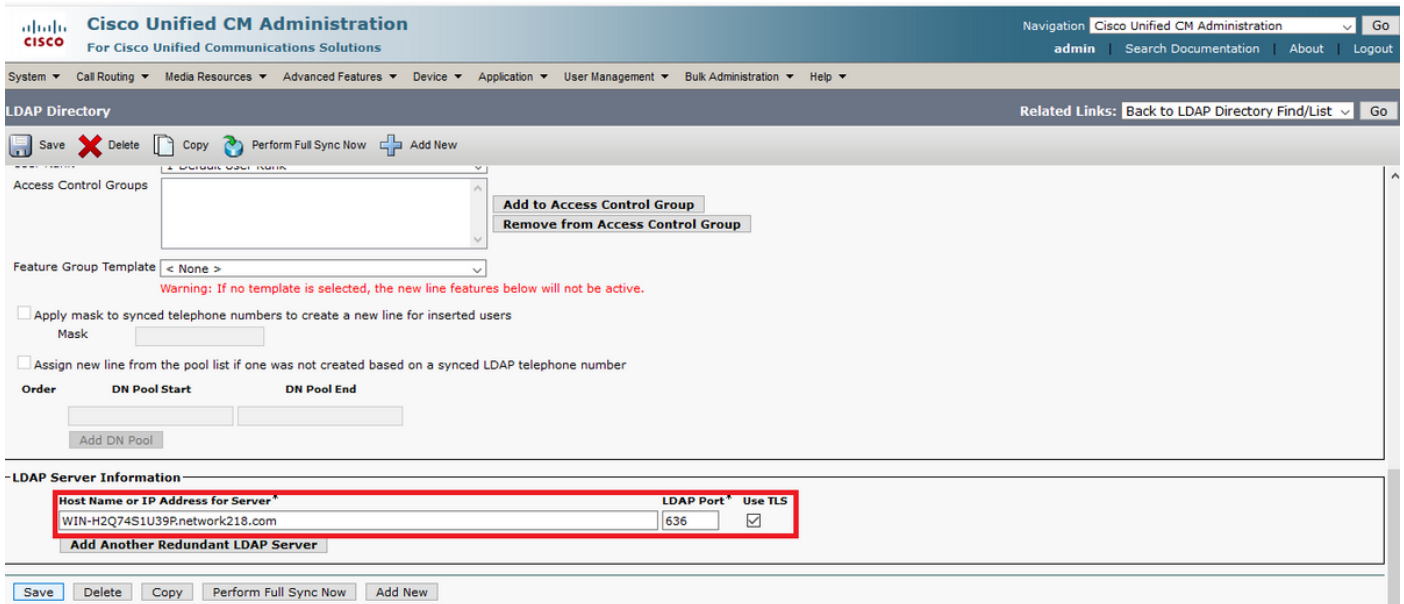
Welcome to the Platform Command Line Interface

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=
```

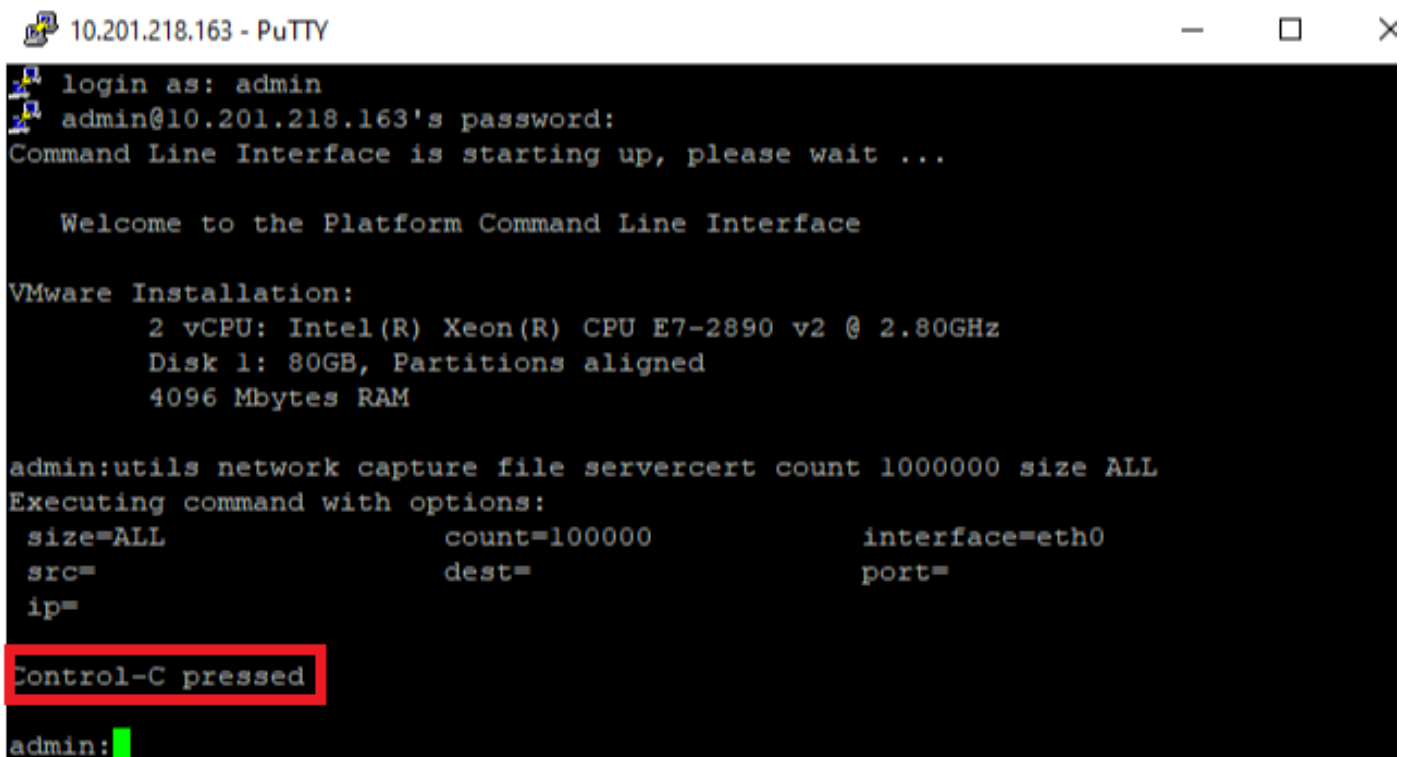
Passaggio 2. Avviare una connessione TLS tra Server e CUCM

In questo esempio, viene avviata una connessione TLS tra un server Secure Lightweight Directory Access Protocol (LDAPS) e CUCM stabilendo una connessione sulla porta TLS 636, come mostrato nell'immagine:



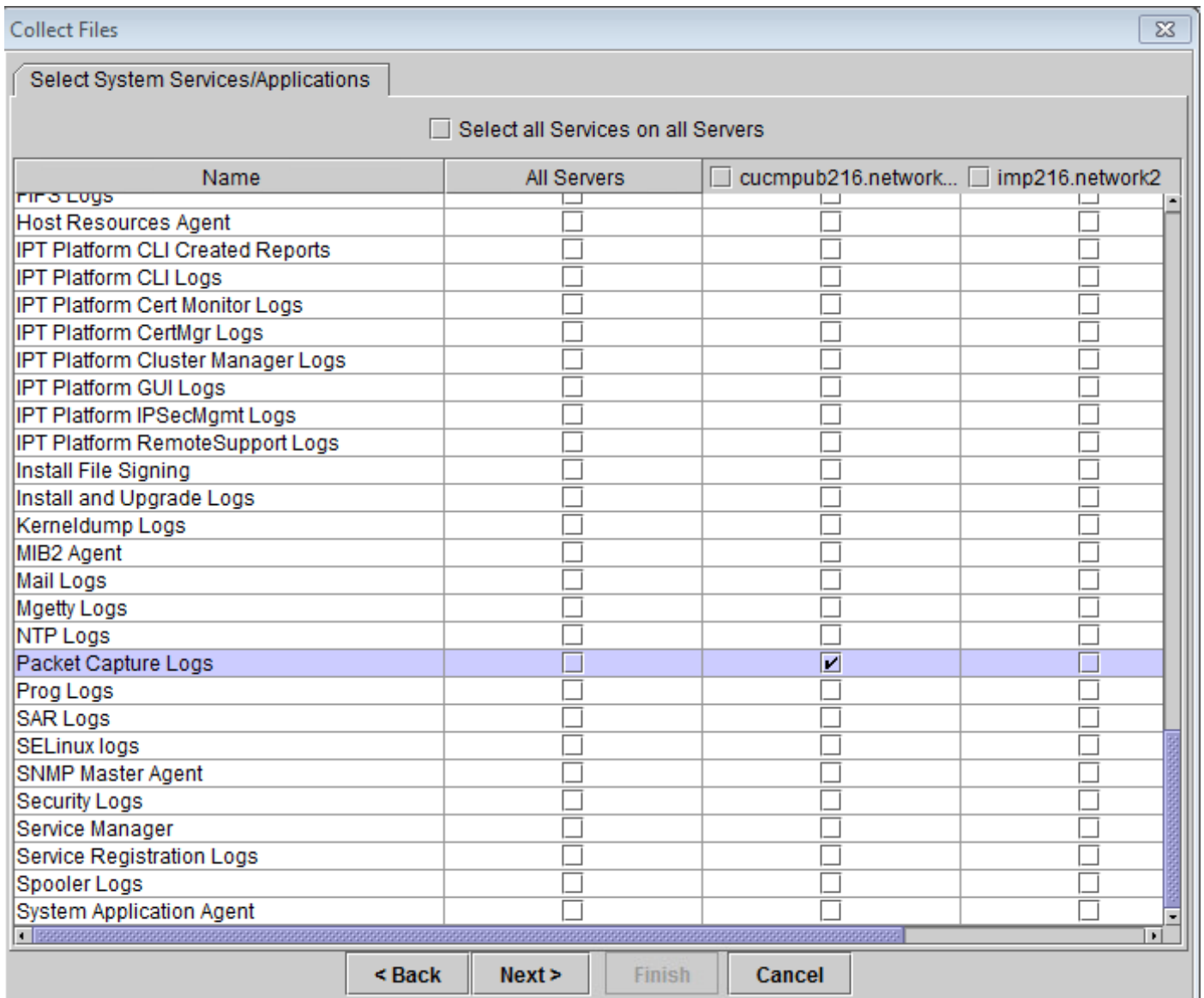
Passaggio 3. Arrestare CUCM PCAP dopo il completamento dell'handshake TLS

Premere **Control-C** per interrompere l'acquisizione del pacchetto, come mostrato nell'immagine



Passaggio 4. Scaricare il file di acquisizione del pacchetto utilizzando uno dei due metodi elencati

1. Avviare RTMT per il nodo CUCM e passare a **Sistema > Strumenti > Traccia > Centro traccia e log > Raccogli file** e selezionare la casella **Registri acquisizione pacchetti** (continuare il processo RTMT per scaricare il pcap), come mostrato nell'immagine:



2. Avviare un server SFTP (Secure File Transport Protocol) e nella sessione SSH CUCM eseguire il file di comando **get activelog /form/cli/<nomefile pac>.cap** (continuare attraverso le richieste per scaricare PCAP sul server SFTP), come mostrato nell'immagine:

```
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

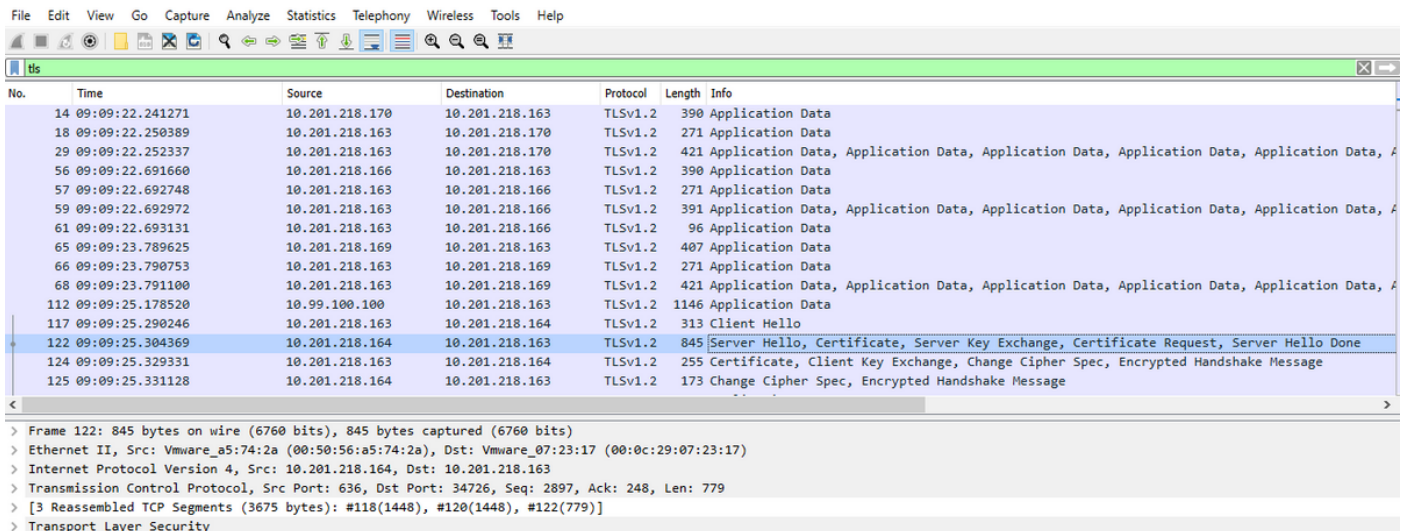
admin:utils network capture file servercert count 1000000 size ALL
Executing command with options:
size=ALL count=100000 interface=eth0
src= dest= port=
ip=

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]? [ ]
```

Passaggio 5. Determinare il numero di certificati presentati a CUCM dal server

Utilizzare l'applicazione Wireshark per aprire il cappuccio e filtrare in base a **tls** per determinare il pacchetto con **Server Hello** contenente la catena di certificati/certificati del server presentata a CUCM. Questo è il fotogramma 122, come mostrato nell'immagine:



·Espandere **Transport Layer Security >Certificate** information dal pacchetto Server Hello con certificato per determinare il numero di certificati presentati a CUCM. Il certificato principale è il certificato del server. In questo caso, viene visualizzato un solo certificato, il certificato server, come illustrato nell'immagine:

The screenshot displays the Wireshark interface with a packet capture of a TLS handshake. The packet list pane shows the following data:

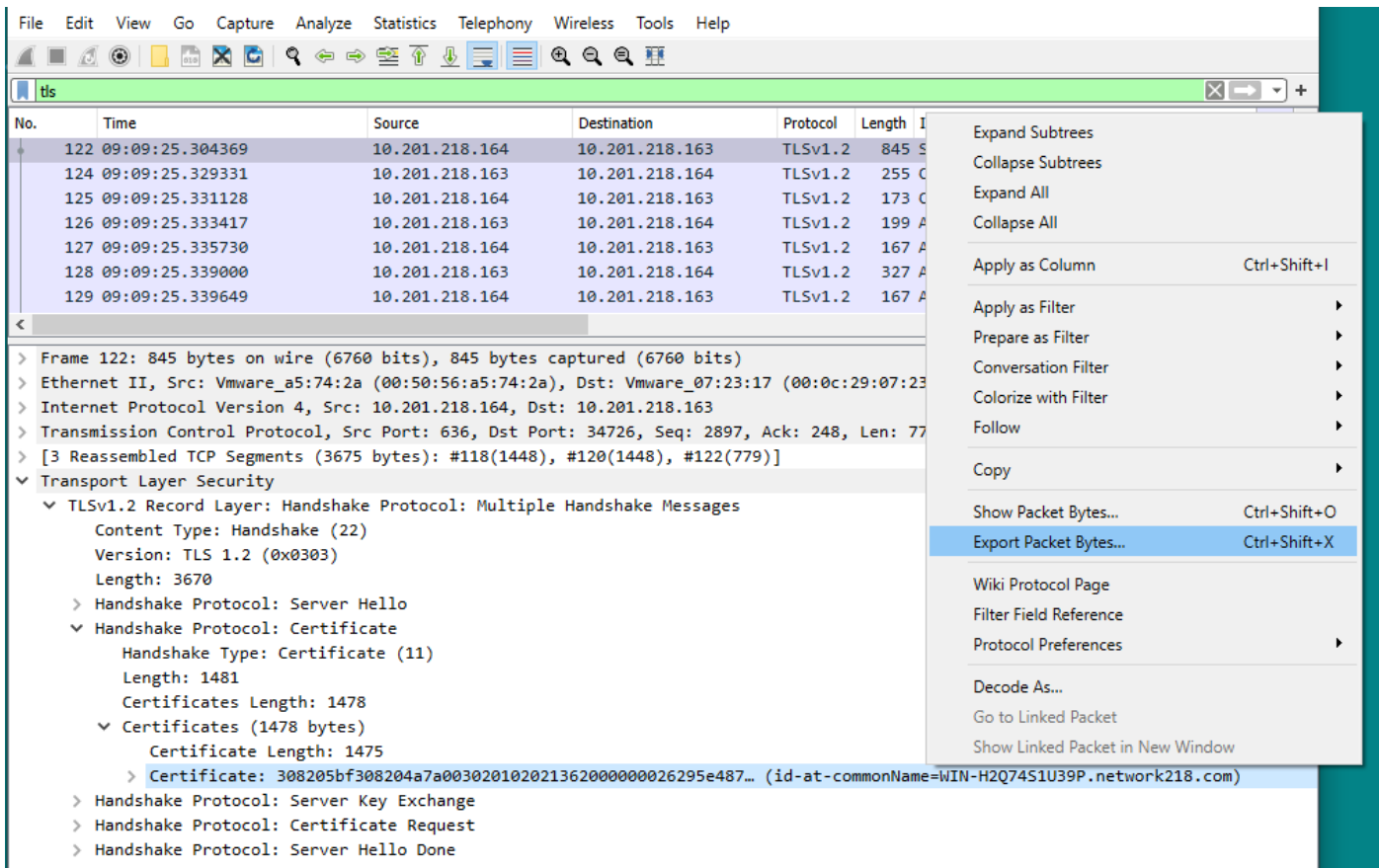
No.	Time	Source	Destination	Protocol	Length	Info
122	09:09:25.304369	10.201.218.164	10.201.218.163	TLSv1.2	845	Server Hello, Certificate, Server K...
124	09:09:25.329331	10.201.218.163	10.201.218.164	TLSv1.2	255	Certificate, Client Key Exchange, C...
125	09:09:25.331128	10.201.218.164	10.201.218.163	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

The packet details pane for frame 122 is expanded to show the following structure:

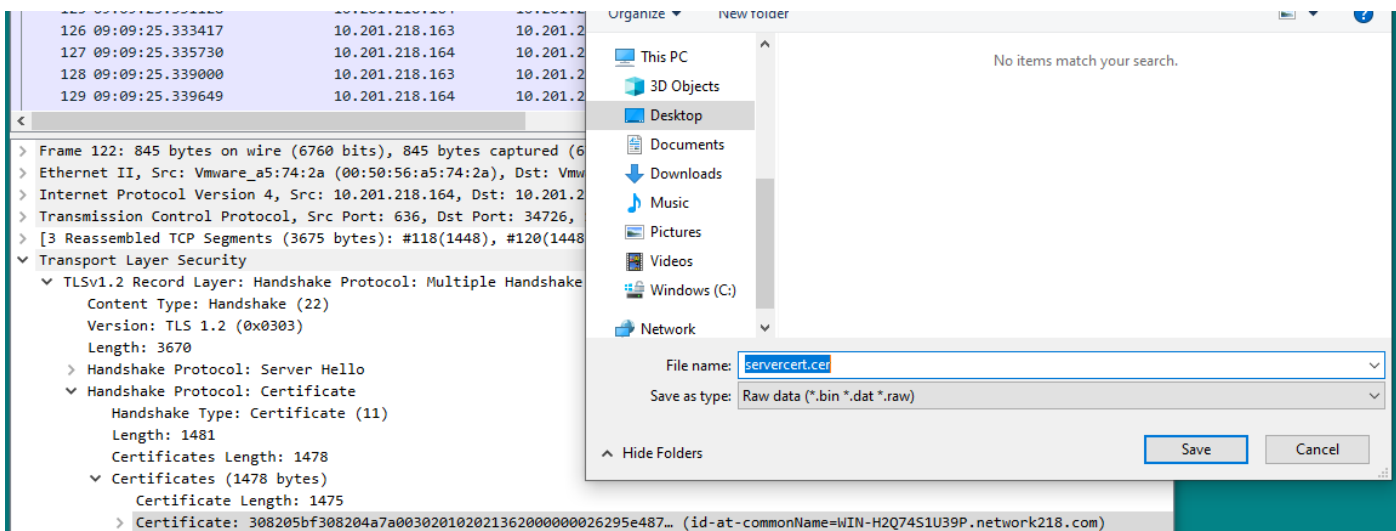
- > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
 - > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)
 - > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163
 - > Transmission Control Protocol, Src Port: 636,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

Passaggio 6. Esportare la catena di certificati/certificati del server dal protocollo PCAP CUCM

In questo esempio viene presentato solo il certificato del server, pertanto è necessario esaminarlo. Fare clic con il pulsante destro del mouse sul certificato del server e selezionare **Export Packet Bytes** (Esporta byte pacchetti) per salvare come certificato con estensione cer, come mostrato nell'immagine:

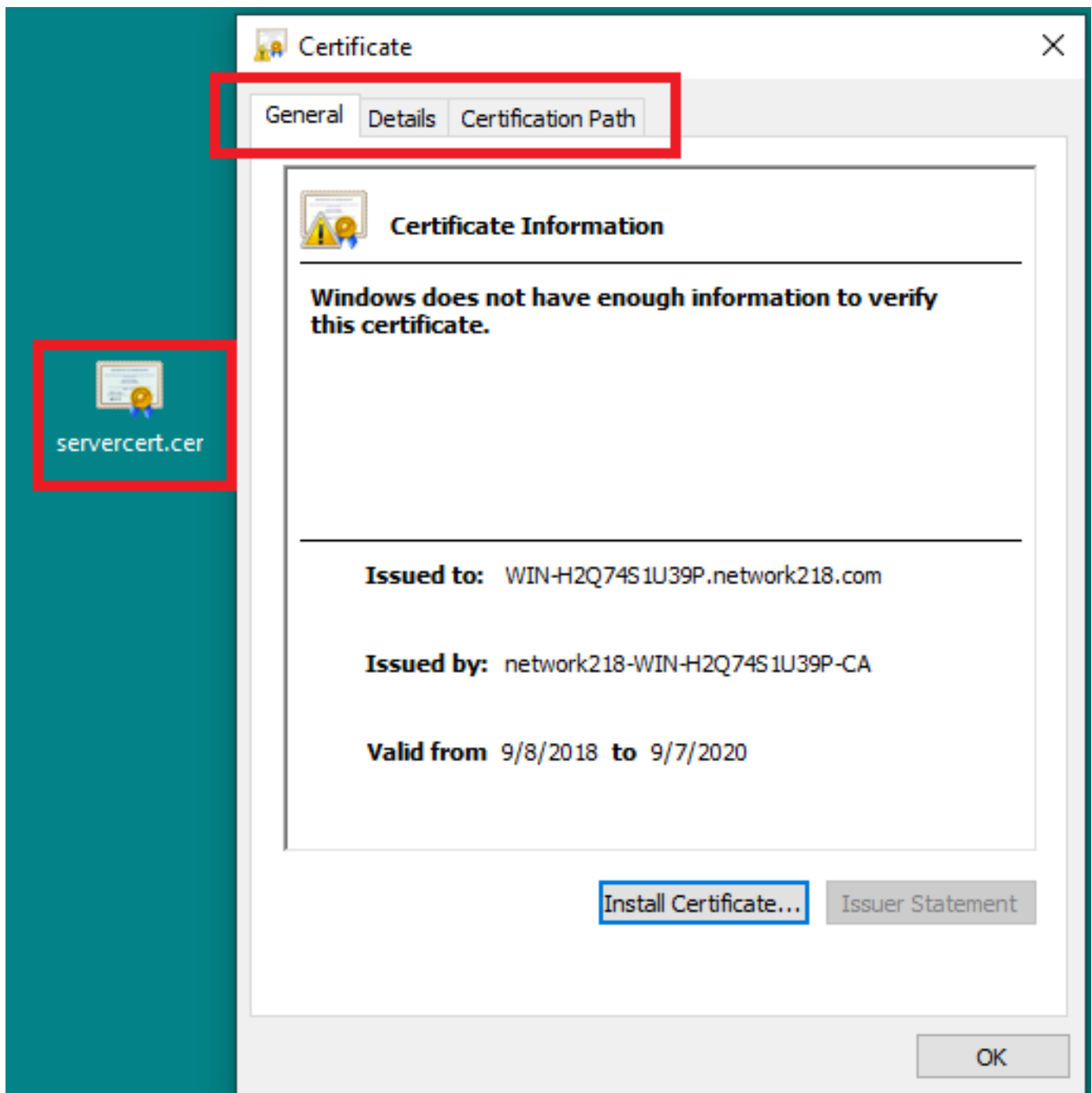


Nella finestra successiva, fornire un nome file con estensione cer e fare clic su Salva. Il file salvato (in questo caso sul desktop) è stato denominato servercert.cer, come mostrato nell'immagine:



Passaggio 7. Aprire il file con estensione CER salvato per esaminarne il contenuto

Fare doppio clic sul file con estensione cer per esaminare le informazioni nelle schede **Generale**, **Dettagli** e **Percorso certificato**, come mostrato nell'immagine:



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.