

Hoe u TLS-certificering kunt exporteren vanuit CUCM Packet Capture (PCAP)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[TLS-certificaat exporteren vanuit CUCM PCAP](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft de procedure om een certificaat uit een Cisco Unified Communications Manager (CUCM) PCAP te exporteren.

Bijgedragen door Adrian Esquillo, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- TelePresence (Transport Layer Security) handdruk
- CUCM-certificaatbeheer
- Secure File Transport Protocol (SFTP) server
- Realtime Monitoring Tool (RTMT)

- Toepassing voor draadloos haaien

Gebruikte componenten

- CUCM release 9.X en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Een server certificaat/certificeringsketen kan worden geëxporteerd om te bevestigen dat de server

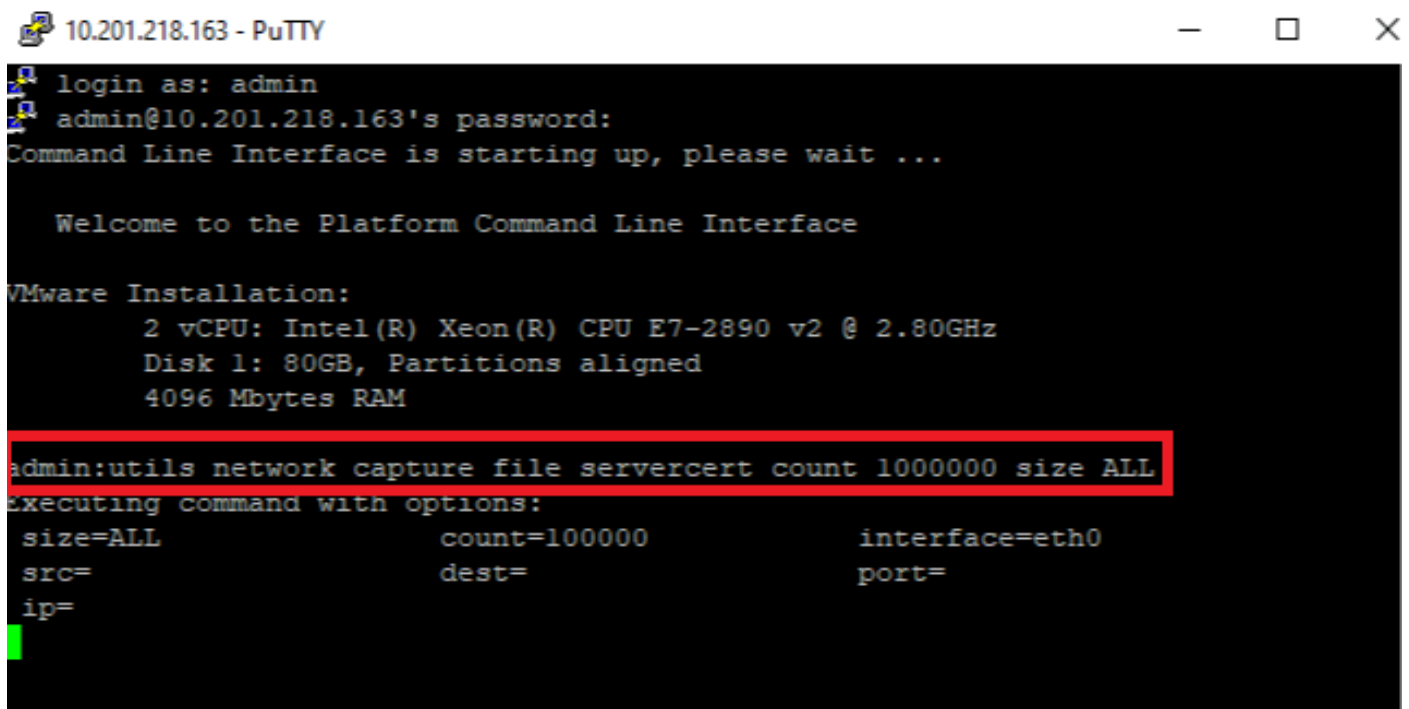
certificaat/certificeringsketen die door de server wordt geleverd, overeenkomt met de te uploaden certificaten of die worden geüpload naar CUCM certificaatbeheer.

Als onderdeel van de TLS-handdruk biedt de server de keten van het servercertificaat aan CUCM.

TLS-certificaat exporteren vanuit CUCM PCAP

Stap 1. Start de pakketvastlegging opdracht op CUCM

Stel een Secure Shell (SSH)-verbinding in op het CUCM-knooppunt en voer het **bestand <filename>** opnamen **van het commando-netwerk uit (of regeren-roteren), alsmede de grootte ALL**, zoals in de afbeelding:



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

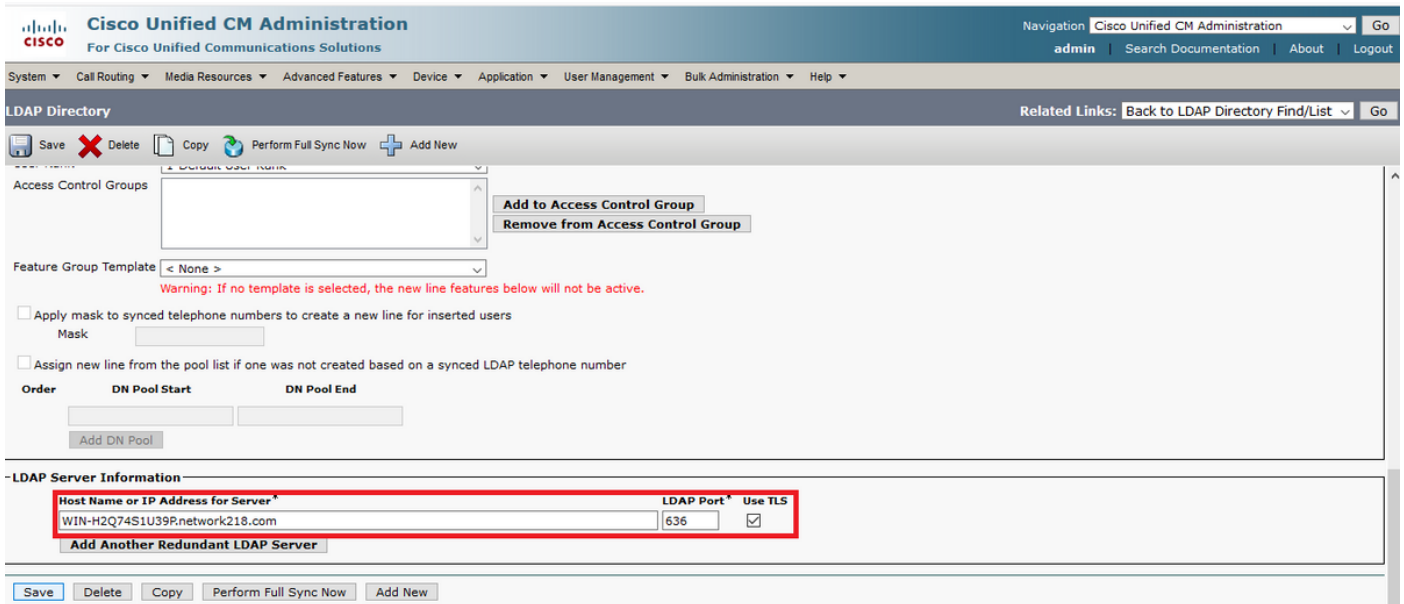
Welcome to the Platform Command Line Interface

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=
```

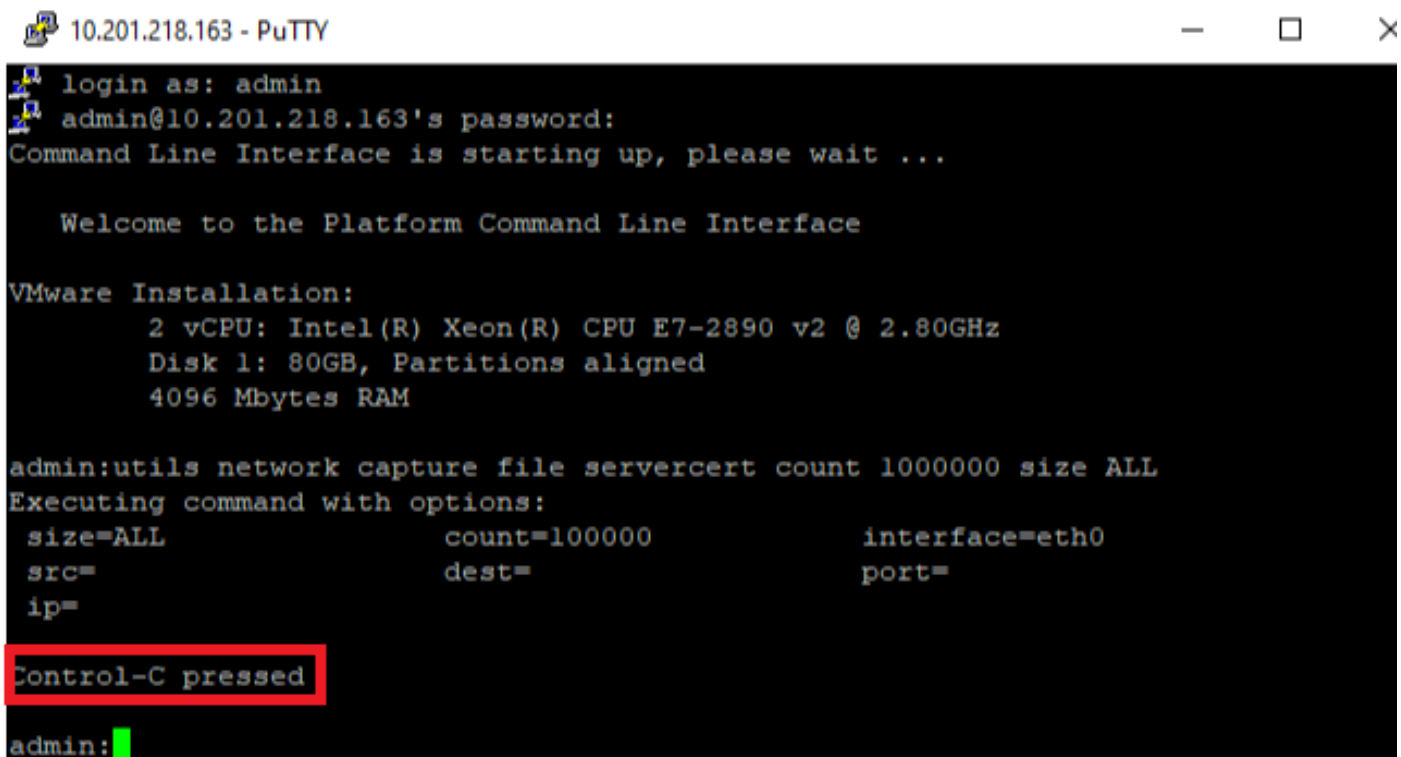
Stap 2. Start een TLS-verbinding tussen Server en CUCM

In dit voorbeeld start u een TLS-verbinding tussen een Secure Lichtgewicht Directory Access Protocol (LDAPS) server en CUCM door een verbinding op TLS poort 636 in te stellen, zoals in de afbeelding wordt getoond:



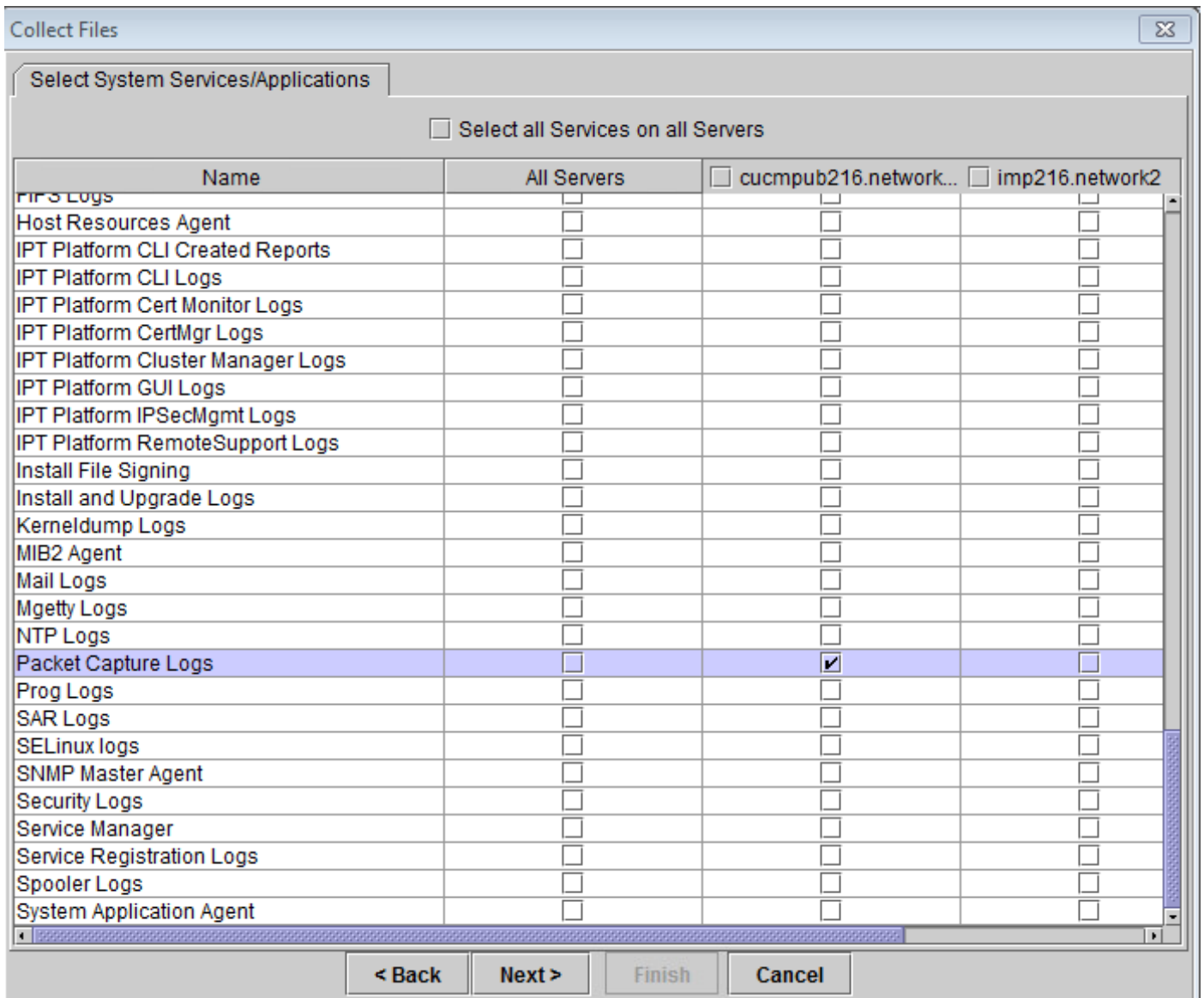
Stap 3. Stop CUCM PCAP nadat de TLS-handdruk is voltooid

Druk op **Control-C** om de pakketvastlegging te stoppen, zoals in de afbeelding



Stap 4. Download het bestand van de pakketvastlegging volgens een van de twee genoemde methoden

1. Start RTMT voor CUCM-knooppunt en navigeer naar **stelsel > Gereedschappen > Zoeken > Centraal overschakelen > Opnemen** en controleer de **Packet Capture Logs** (ga door het RTMT-proces om het pad te downloaden), zoals in de afbeelding te zien is:



2. Start een Secure File Transport Protocol (SFTP) server en voer in de CUCM SSH-sessie het opdrachtbestand activeren/patform/cli/<pcap filename>.cap (doorgaan met de aanwijzingen om het PCAP op SFTP-server te downloaden), zoals in de afbeelding wordt weergegeven:

```

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=

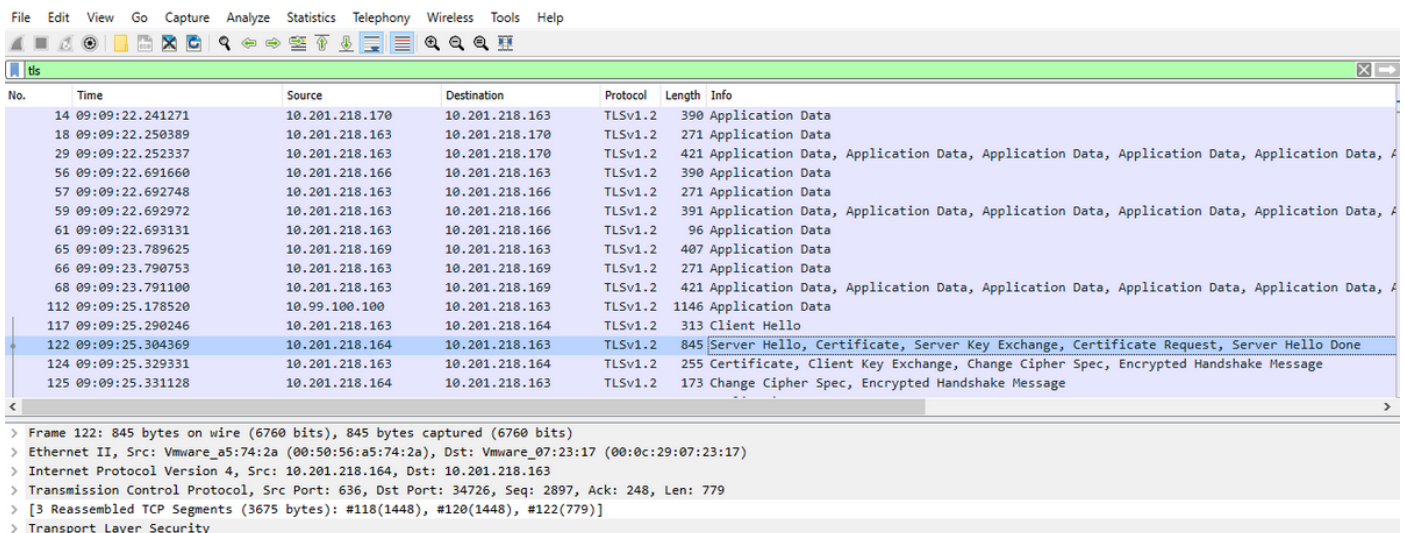
Control-C pressed

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]? [ ]

```

Stap 5. Bepaal het aantal certificaten dat door de server aan CUCM wordt aangeboden

Gebruik de toepassing Wireless-shark om het deksel en het filter op **tls** te openen om het pakket met **server Hallo** te bepalen dat de aan CUCM aangeboden server certificaat/certificeringsketen bevat. Dit is frame 122, zoals in de afbeelding weergegeven:



- Uitbreidt de **Beveiliging van de transportlaag** > **certificaat** informatie uit het pakket van de Server Hallo met certificaat om het aantal certificaten te bepalen dat aan CUCM wordt aangeboden. Het hoogste certificaat is het servercertificaat. In dit geval wordt slechts 1 certificaat, het servercertificaat, gepresenteerd zoals in de afbeelding:

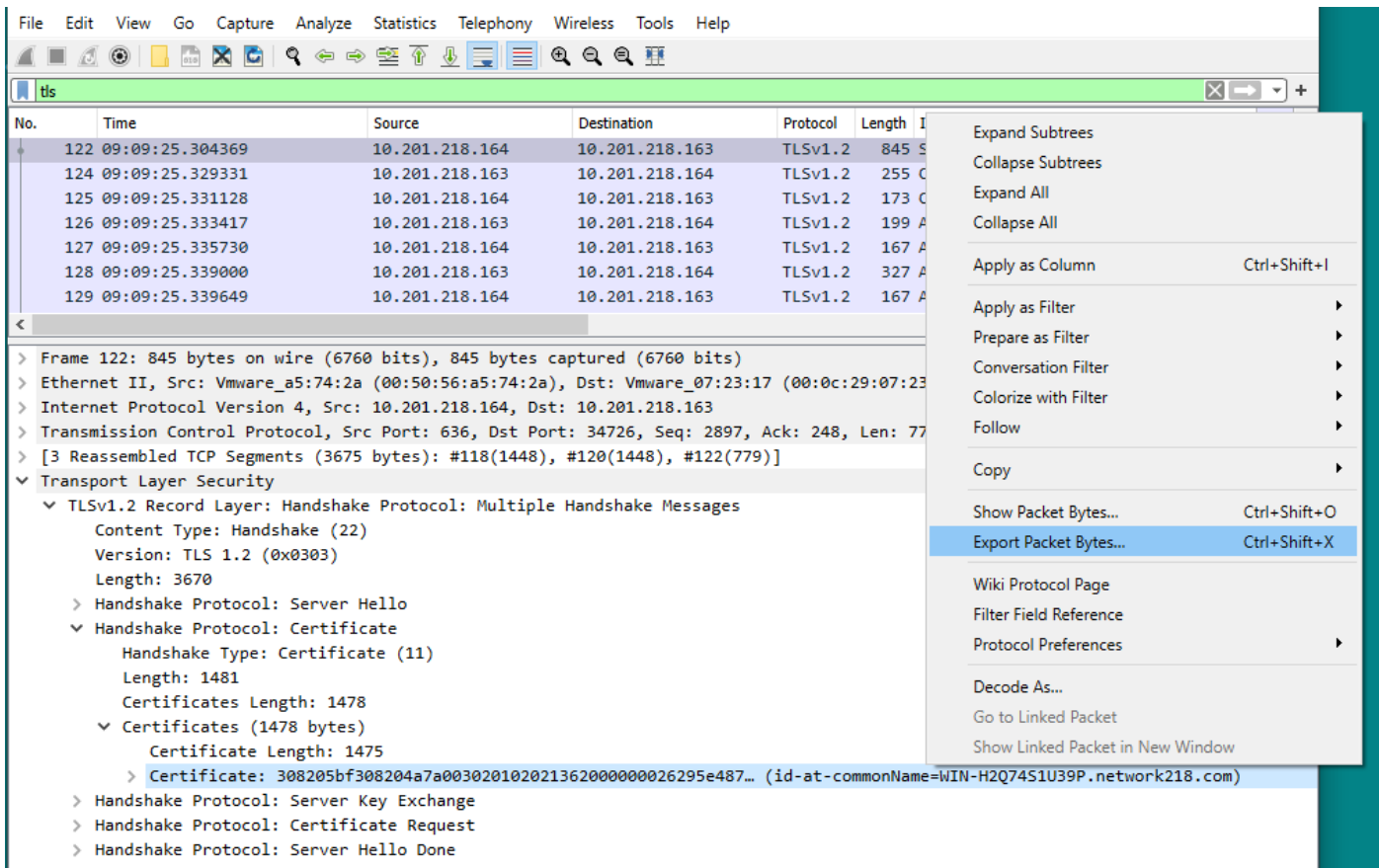
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

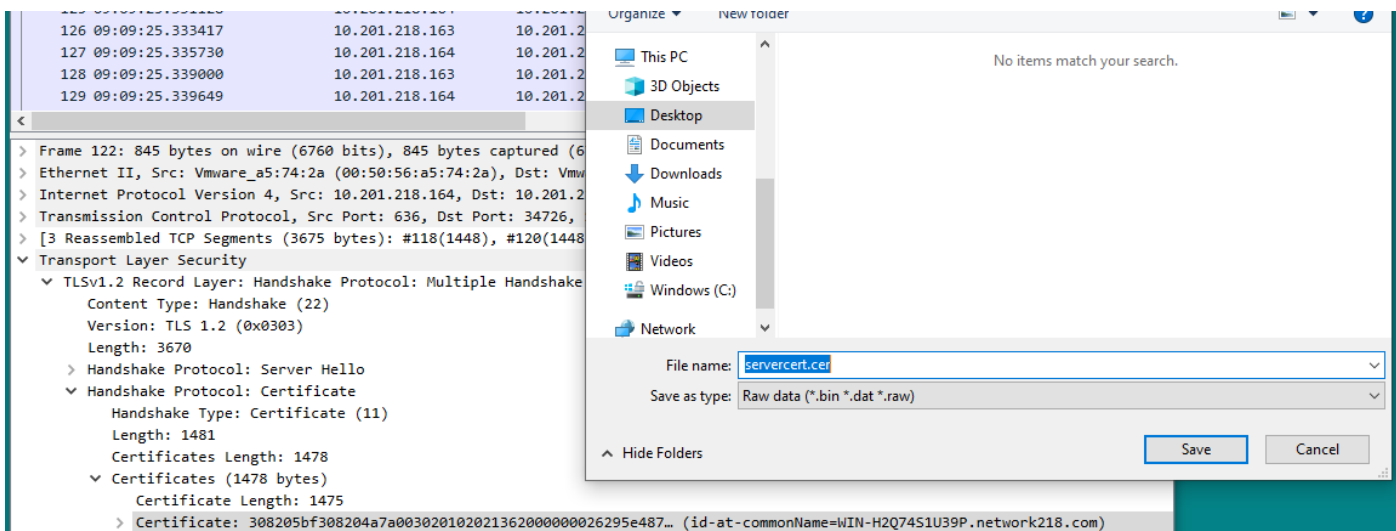
- > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
- > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)
- > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163
- > Transmission Control Protocol, Src Port: 636,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

Stap 6. Exporteren van het servercertificaat/de certificeringsketen uit de CUCM PCAP

In dit voorbeeld wordt alleen het servercertificaat weergegeven. U dient het servercertificaat dus te onderzoeken. Klik met de rechtermuisknop op het servercertificaat en selecteer **Packet Bytes exporteren** om op te slaan als .cer-certificaat, zoals weergegeven in de afbeelding:

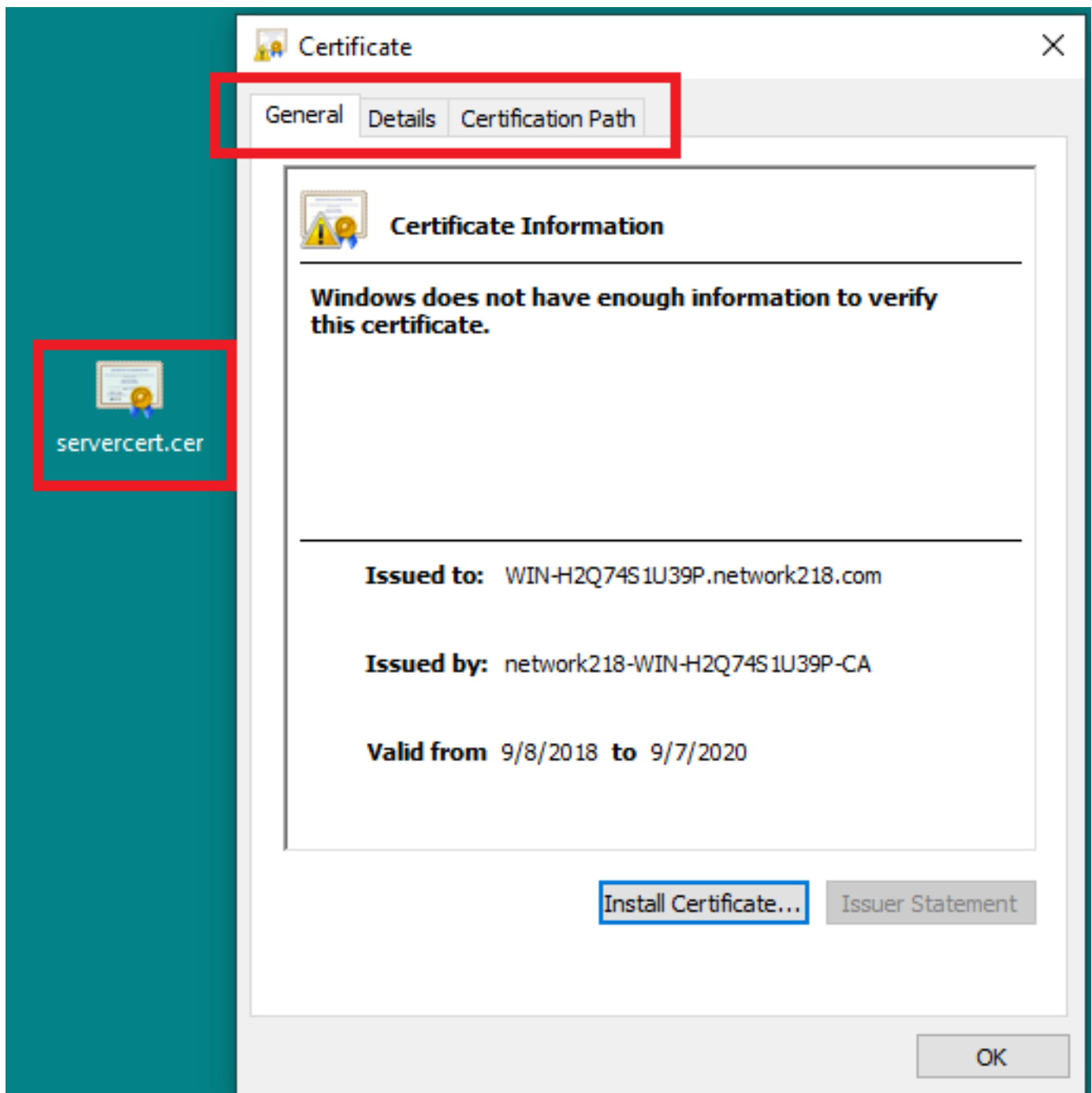


• Typ in het volgende venster een .cer-bestandsnaam en klik vervolgens op Opslaan. Het bestand dat werd opgeslagen (in dit geval naar het bureaublad) werd server cert.cer genoemd, zoals in de afbeelding weergegeven:



Stap 7. Open het opgeslagen CER-bestand om de inhoud te onderzoeken

Dubbelklik op het .cer-bestand om de informatie te onderzoeken in de tabbladen **Algemeen**, **Details** en **certificaatpad**, zoals in de afbeelding weergegeven:



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.