

Exportieren der TLS-Zertifizierung aus CUCM Packet Capture (PCAP)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[TLS-Zertifikat vom CUCM PCAP exportieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt das Verfahren zum Exportieren eines Zertifikats von einem Cisco Unified Communications Manager (CUCM) PCAP.

Mitarbeiter: Adrian Esquillo, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Transport Layer Security (TLS)-Handshake
- CUCM-Zertifikatsverwaltung
- Secure File Transport Protocol (SFTP)-Server
- Realtime Monitoring Tool (RTMT)

Wireshark-Anwendung

Verwendete Komponenten

- CUCM Version 9.X oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ein Serverzertifikat/eine Zertifikatkette kann exportiert werden, um zu bestätigen, dass das vom

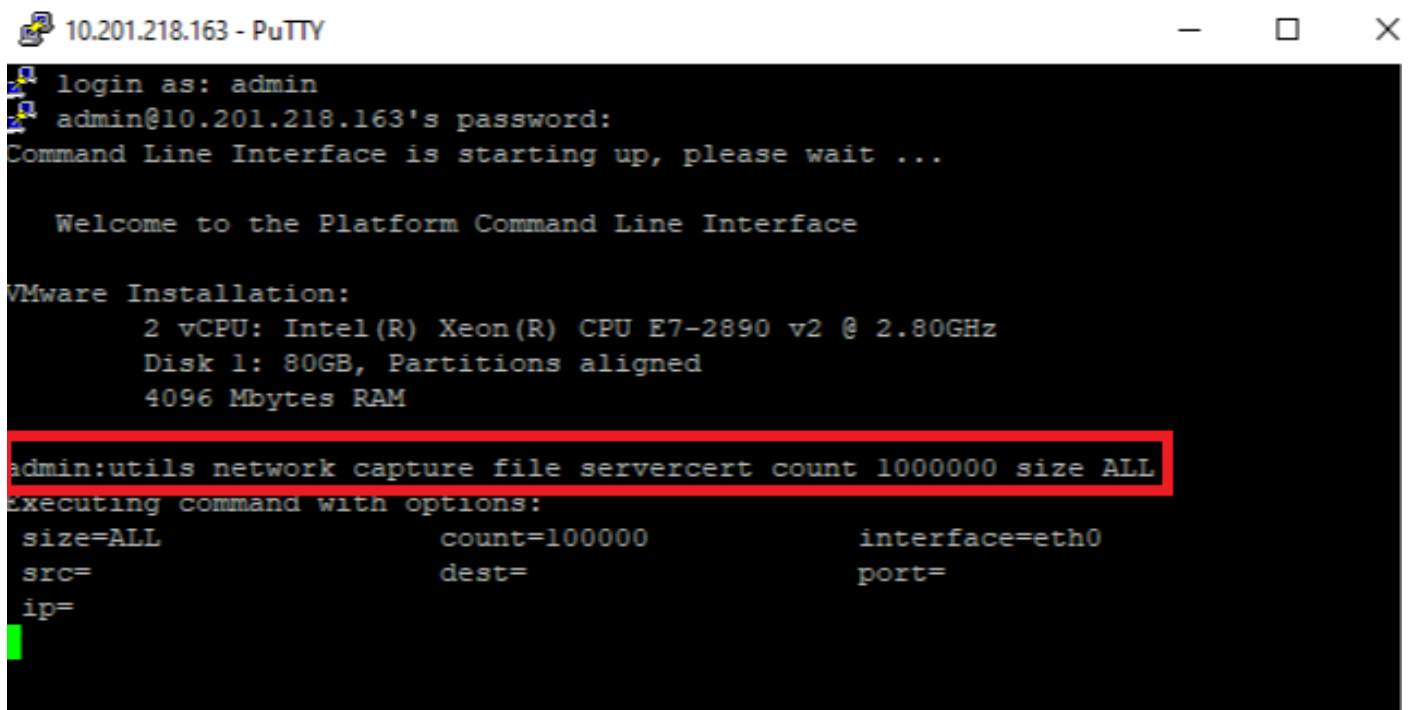
Server bereitgestellte Serverzertifikat/die vom Server bereitgestellte Zertifikatkette mit den hochzuladenden Zertifikaten übereinstimmt oder in das CUCM-Zertifikatsmanagement hochgeladen wird.

Im Rahmen des TLS-Handshake stellt der Server seine Serverzertifikat-/Zertifikatkette für CUCM bereit.

TLS-Zertifikat vom CUCM PCAP exportieren

Schritt 1: Starten des Befehls zur Paketerfassung auf CUCM

Stellen Sie eine Secure Shell (SSH)-Verbindung zum CUCM-Knoten her, und führen Sie den Befehl `utils network capture (or capture-rotation) file <Dateiname> count 100000 size ALL` aus, wie im Bild gezeigt:



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

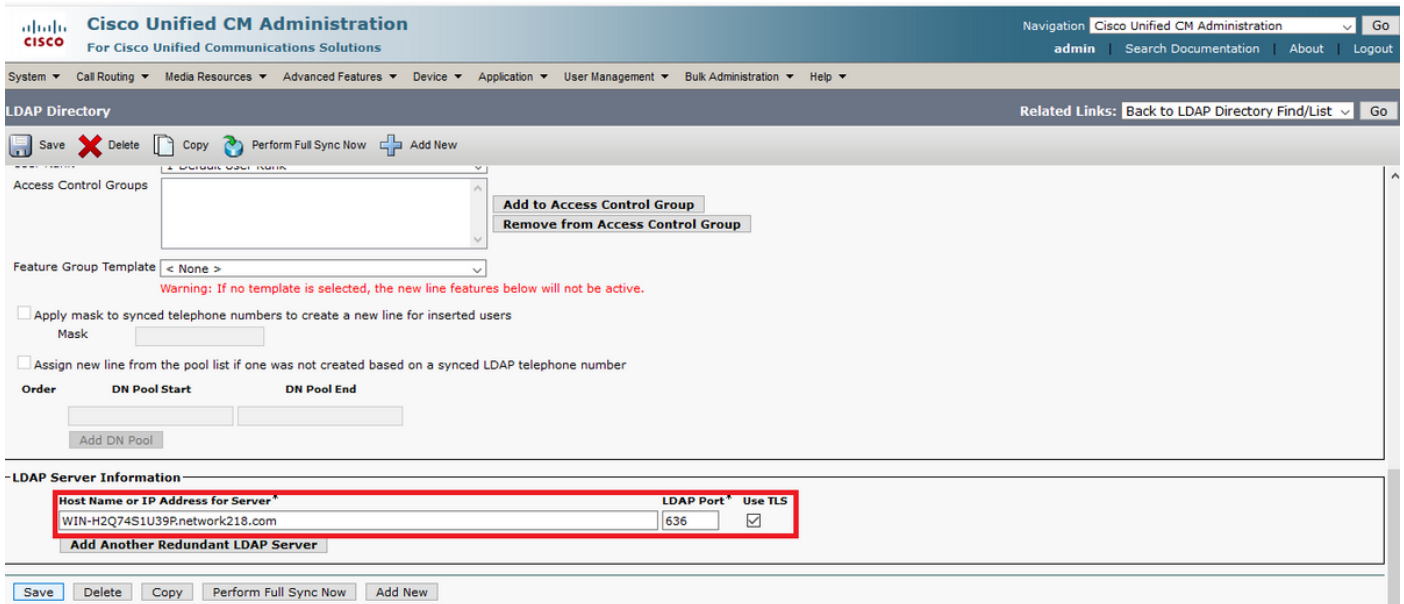
Welcome to the Platform Command Line Interface

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=
```

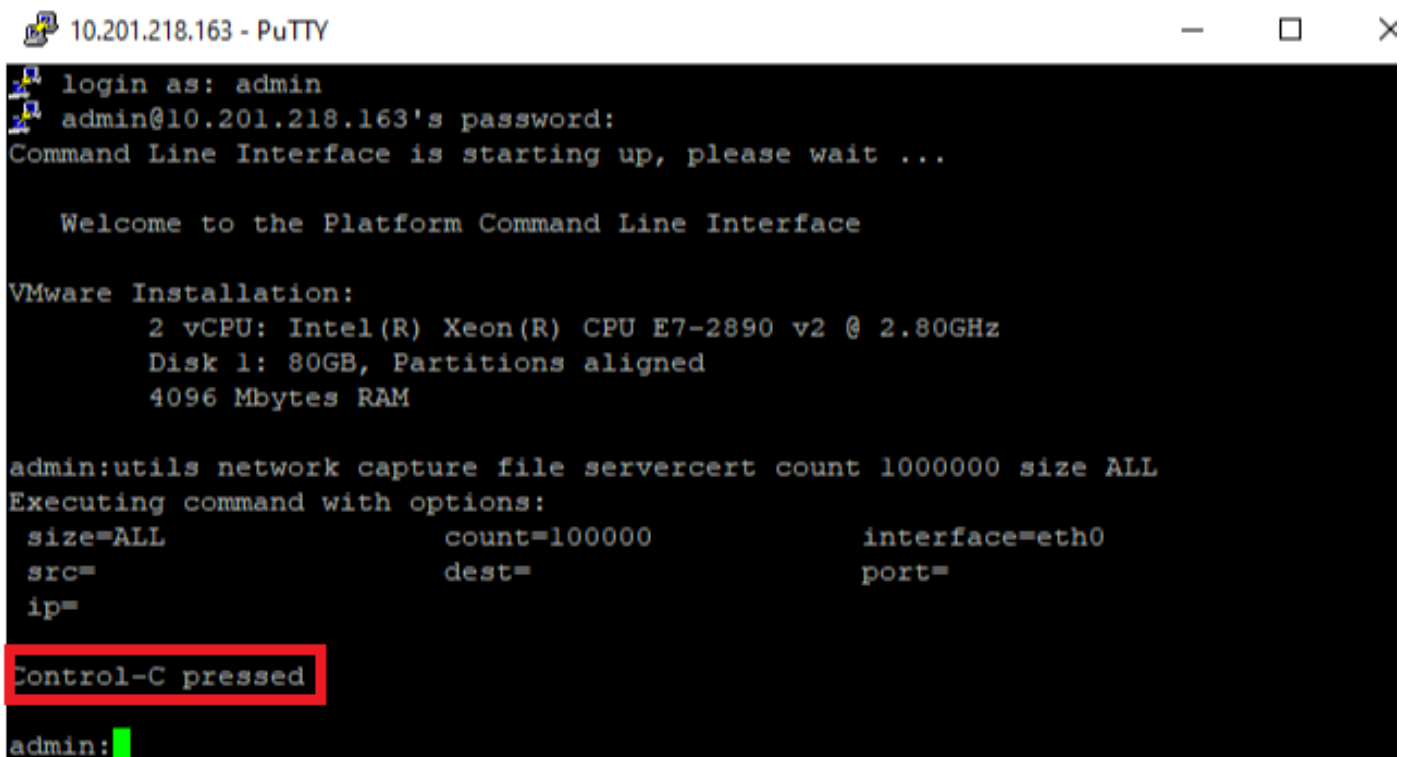
Schritt 2: TLS-Verbindung zwischen Server und CUCM starten

In diesem Beispiel starten Sie eine TLS-Verbindung zwischen einem LDAPS-Server (Secure Lightweight Directory Access Protocol) und dem CUCM, indem Sie eine Verbindung auf dem TLS-Port 636 herstellen, wie im Bild gezeigt:



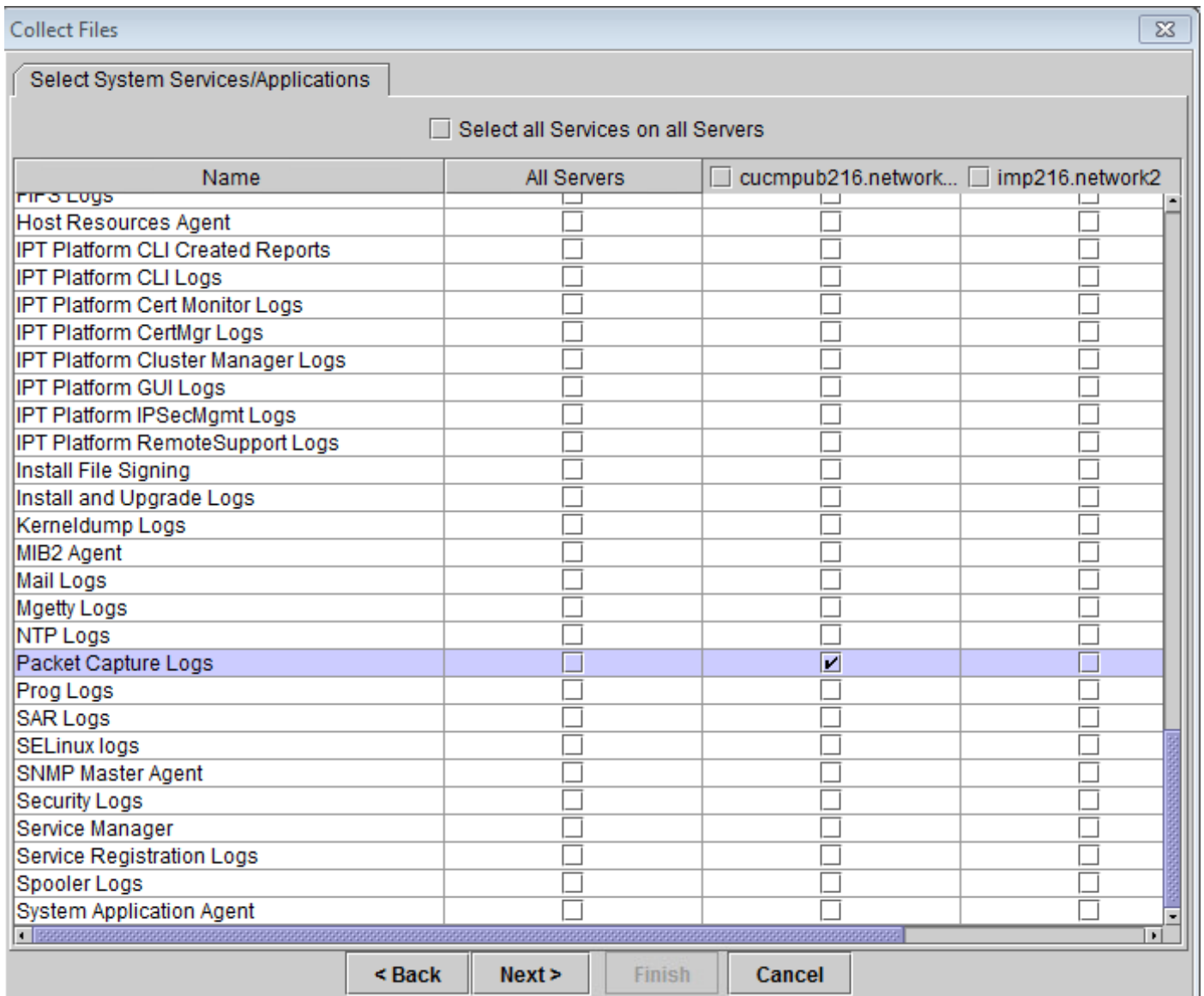
Schritt 3: CUCM-PCAP stoppen, nachdem der TLS-Handshake abgeschlossen ist

Drücken Sie **Control-C**, um die Paketerfassung zu stoppen, wie im Bild gezeigt.



Schritt 4: Laden Sie die Paketerfassungsdatei mit einer der beiden aufgeführten Methoden herunter

1. Starten Sie RTMT für den CUCM-Knoten, navigieren Sie zu **System > Tools > Trace > Trace & Log Central > Collect Files** und aktivieren Sie das Feld **Packet Capture Logs** (fahren Sie mit dem RTMT-Prozess fort, um die pcap-Datei herunterzuladen), wie im Bild gezeigt:



2. Starten Sie einen SFTP-Server (Secure File Transport Protocol), und führen Sie in der CUCM SSH-Sitzung die **Befehlsdatei get activelog /patform/cli/<pcap filename>.cap aus** (fahren Sie mit den Aufforderungen fort, um den PCAP auf dem SFTP-Server herunterzuladen), wie im Bild gezeigt:

```
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

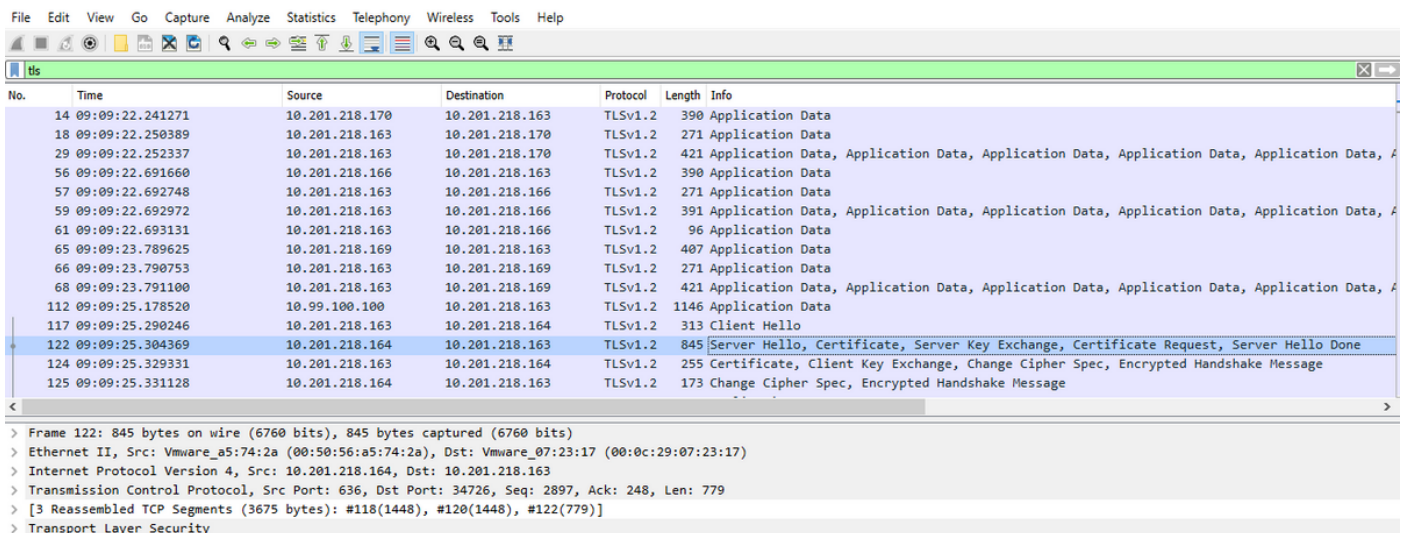
admin:utils network capture file servercert count 1000000 size ALL
Executing command with options:
  size=ALL          count=100000          interface=eth0
  src=              dest=              port=
  ip=

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]? [ ]
```

Schritt 5: Bestimmen Sie die Anzahl der Zertifikate, die der Server dem CUCM vorlegt.

Verwenden Sie die Anwendung Wireshark, um die pcap-Datei zu öffnen und auf **tls** zu filtern, um das Paket mit **Server Hello** zu ermitteln, das das dem CUCM präsentierte Serverzertifikat/Zertifikatskette enthält. Dies ist Frame 122, wie im Bild gezeigt:



erweitern Sie die Informationen **Transport Layer Security > Certificate** vom Server Hello-Paket mit dem Zertifikat, um die Anzahl der Zertifikate zu bestimmen, die dem CUCM vorgelegt werden. Das oberste Zertifikat ist das Serverzertifikat. In diesem Fall wird nur ein Zertifikat, das Serverzertifikat, wie im Bild gezeigt angezeigt:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

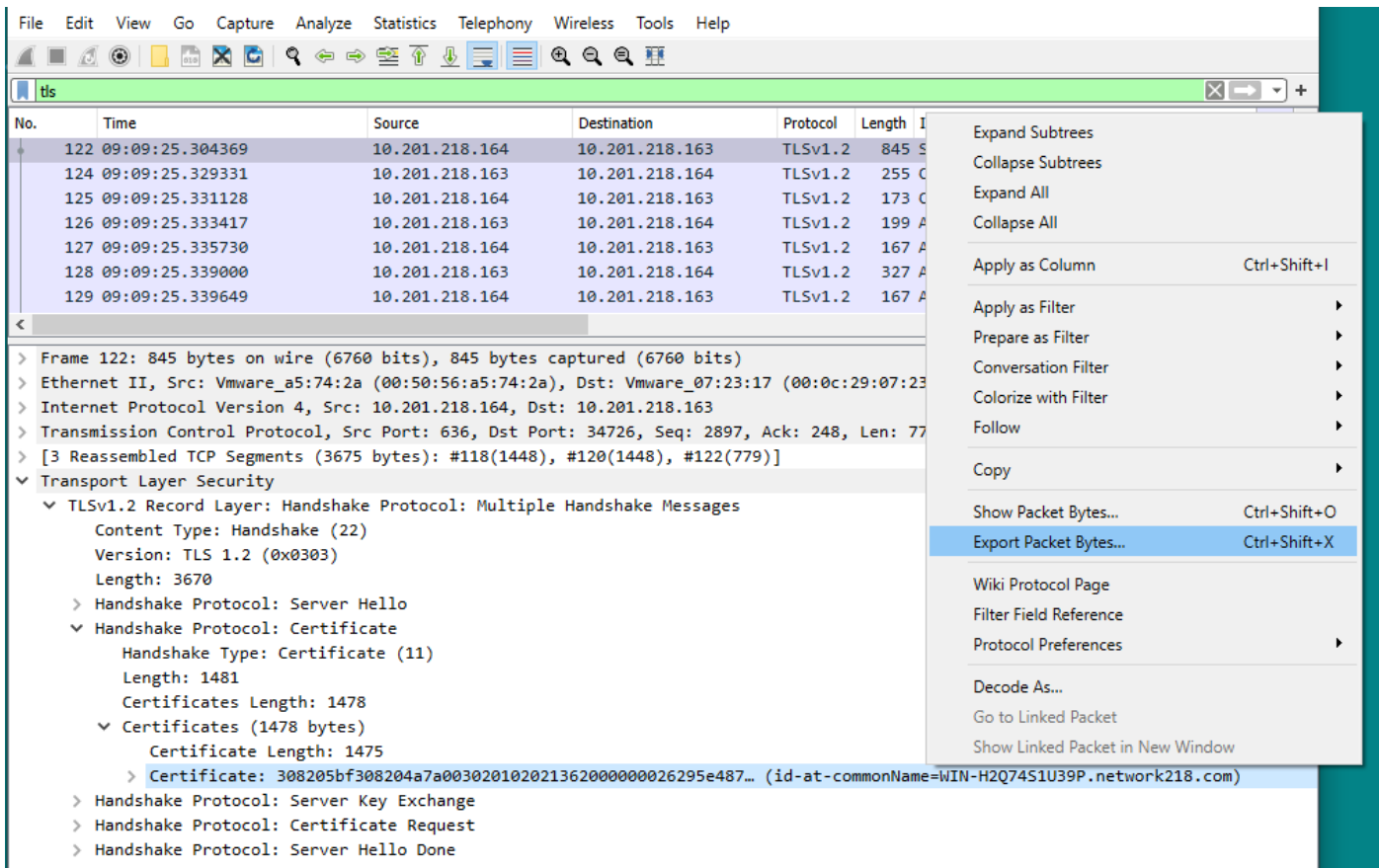
tls

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

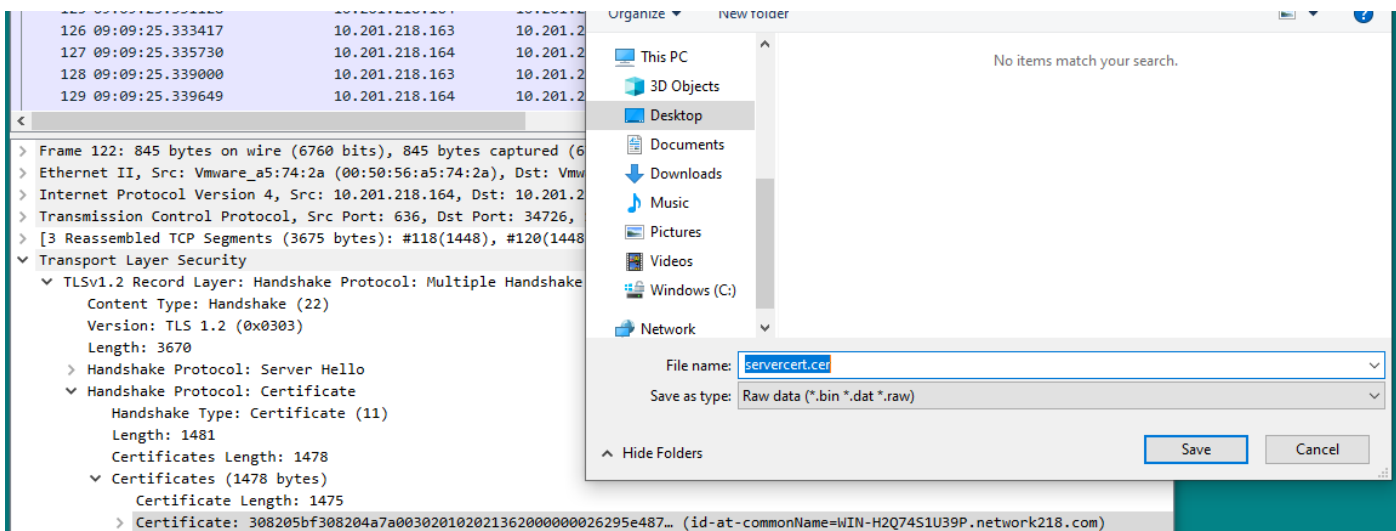
- > Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6760 bits)
- > Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmware_07:23:17 (00:0c:29:07:23:17)
- > Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.218.163
- > Transmission Control Protocol, Src Port: 636,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

Schritt 6: Exportieren des Serverzertifikats/der Zertifikatkette aus dem CUCM PCAP

In diesem Beispiel wird nur das Serverzertifikat angezeigt, daher müssen Sie das Serverzertifikat überprüfen. Klicken Sie mit der rechten Maustaste auf das Serverzertifikat, und wählen Sie **Packet Bytes exportieren aus**, um als .cer-Zertifikat zu speichern, wie im Bild gezeigt:

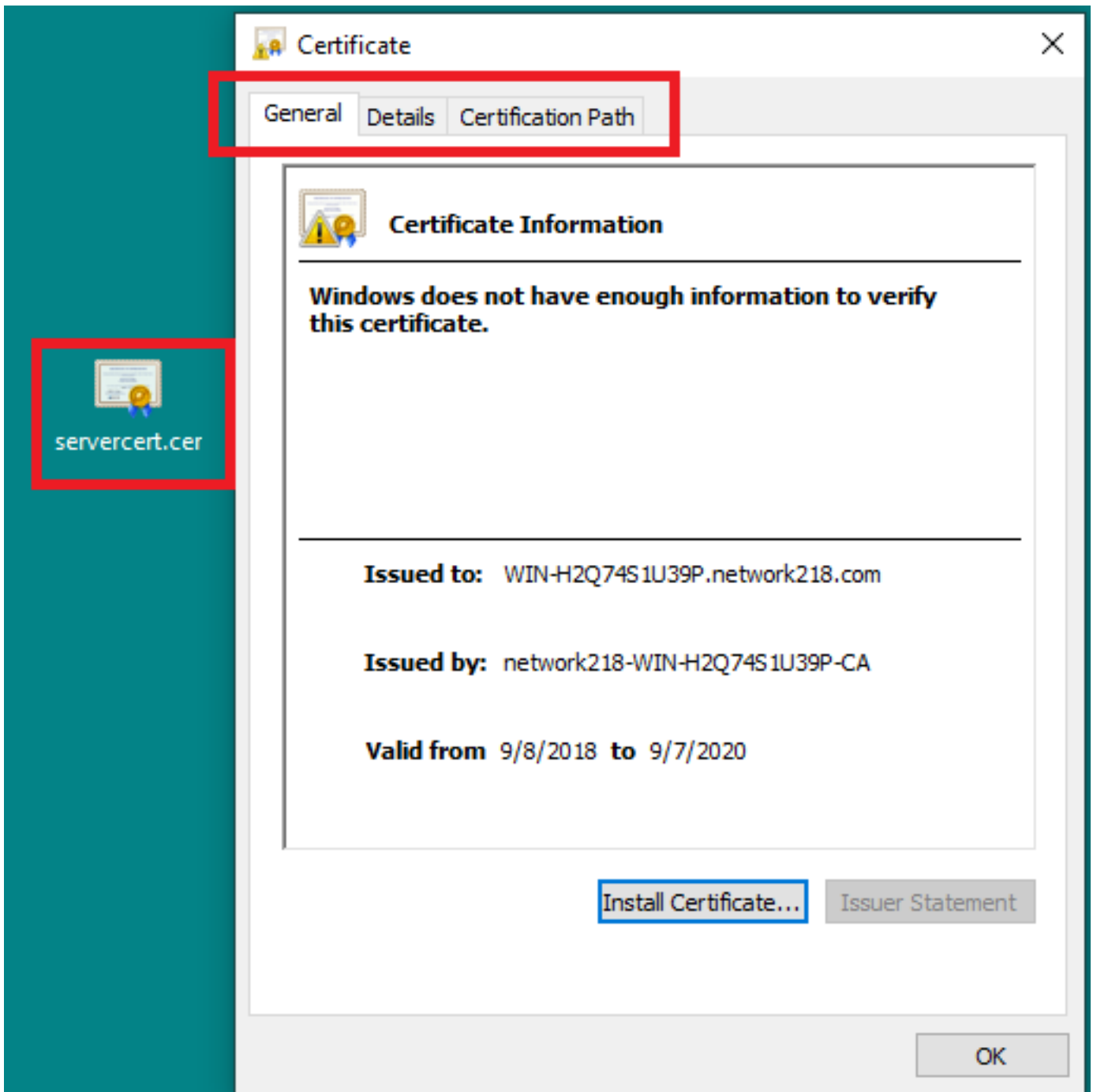


Geben Sie im nachfolgenden Fenster einen Namen für die Cer-Datei an, und klicken Sie dann auf Speichern. Die Datei, die (in diesem Fall auf dem Desktop) gespeichert wurde, wurde ServerCert.cer genannt, wie im Bild gezeigt:



Schritt 7: Öffnen Sie die gespeicherte CER-Datei, um Inhalte zu prüfen.

Doppelklicken Sie auf die Datei .cer, um die Informationen in den Registerkarten **Allgemein**, **Details** und **Zertifikatspfad** zu überprüfen, wie im Bild gezeigt:



Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.