CUCMパケットキャプチャ(PCAP)からTLS証明書をエクスポートする方法

内容

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)PCAPから証明書をエクスポートする手順について説明します。

著者：Cisco TACエンジニア、Adrian Esquillo

前提条件

要件

次の項目に関する知識があることが推奨されます。
・ Transport Layer Security(TLS)ハンドシェイク
・ CUCM証明書管理
・ セキュアファイル転送プロトコル(SFTP)サーバ
・ リアルタイム監視ツール(RTMT)

・ Wiresharkアプリケーション

使用するコンポーネント

・ CUCMリリース9.X以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

サーバ証明書/証明書チェーンは、サーバから提供されたサーバ証明書/証明書チェーンが、アップ

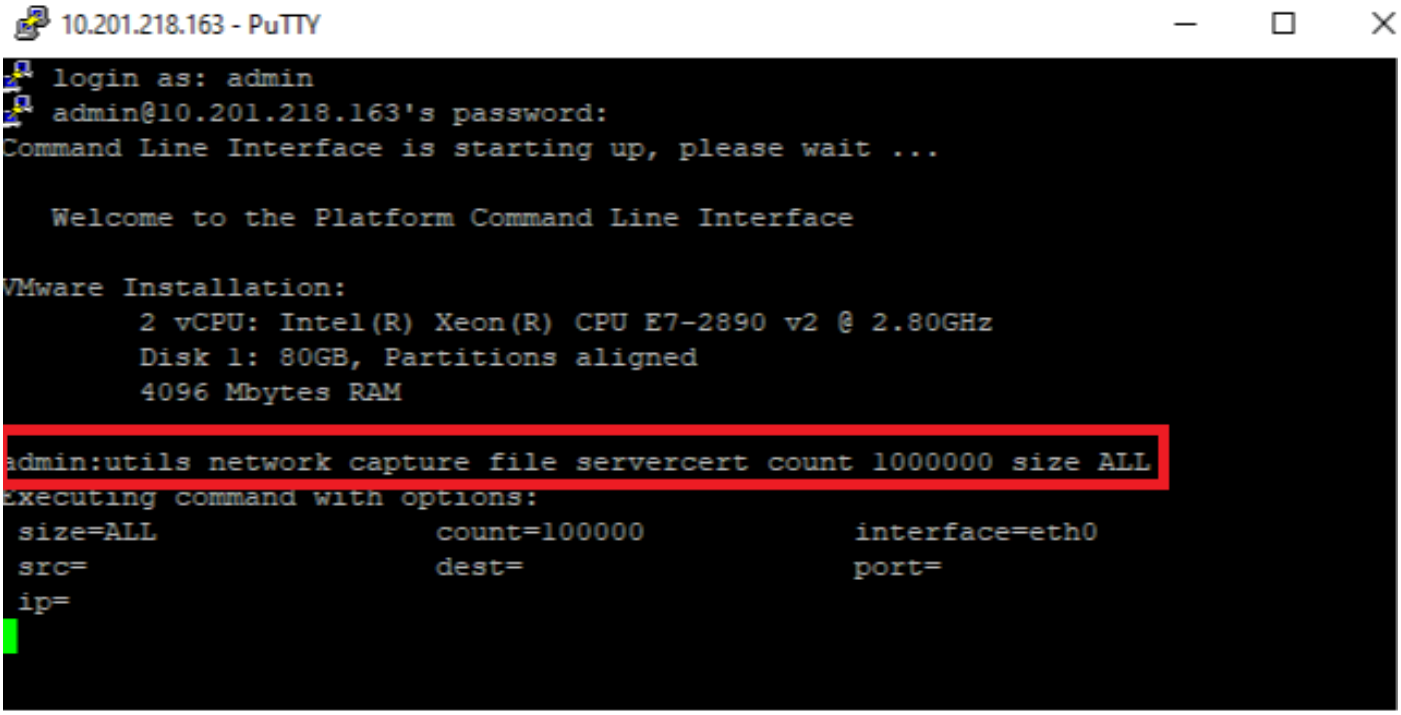
ロードする証明書またはCUCM証明書管理にアップロードされた証明書と一致することを確認するためにエクスポートできます。

TLSハンドシェイクの一部として、サーバはサーバ証明書/証明書チェーンをCUCMに提供します。

CUCM PCAPからのTLS証明書のエクスポート

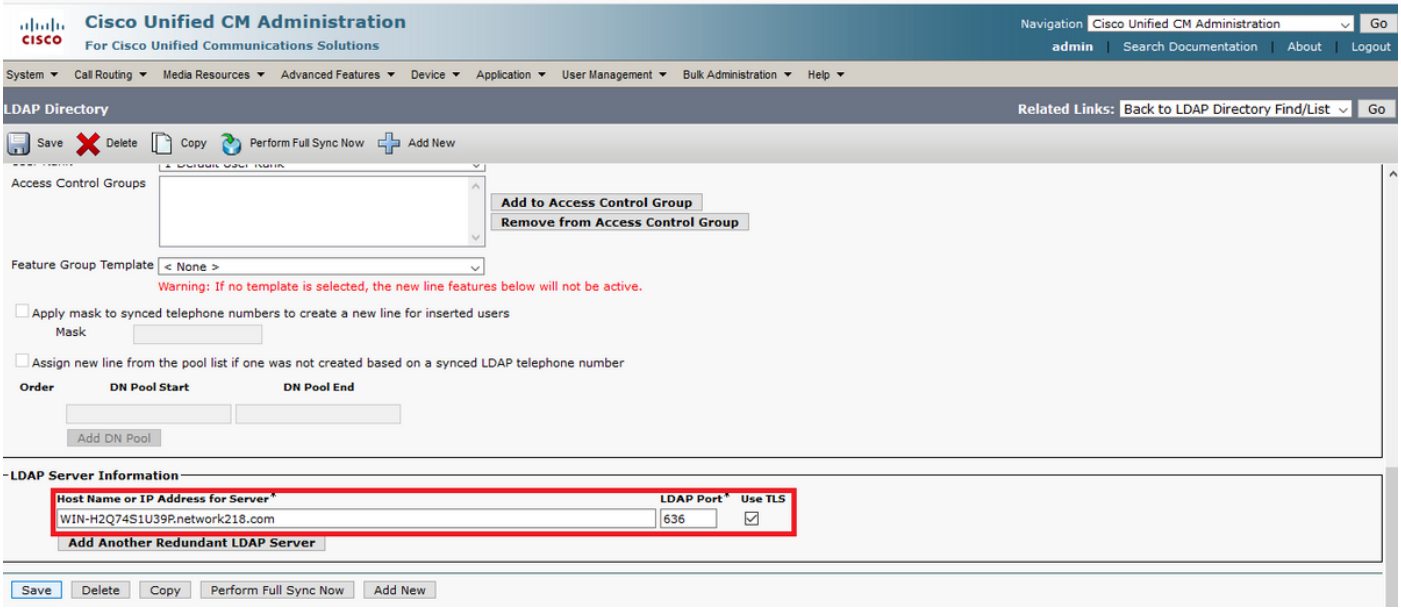
ステップ1:CUCMでpacket captureコマンドを開始します

CUCMノードへのセキュアシェル(SSH)接続を確立し、図に示すように、**utils network capture (or capture-rotate) file <filename> count 1000000 size ALLコマンドを実行します**。



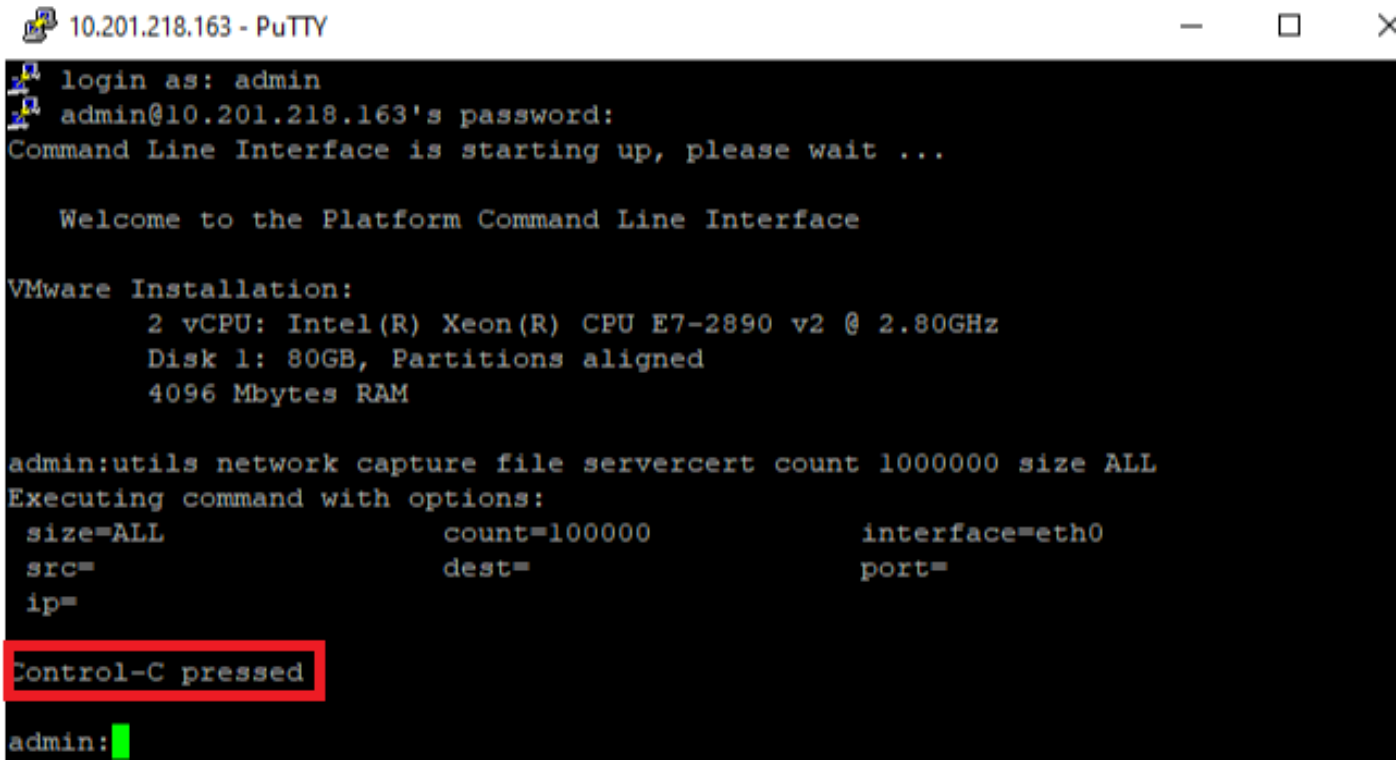
ステップ2：サーバとCUCM間のTLS接続を開始します

この例では、図に示すように、TLSポート636で接続を確立することで、Secure Lightweight Directory Access Protocol(LDAPS)サーバとCUCM間のTLS接続を開始します。



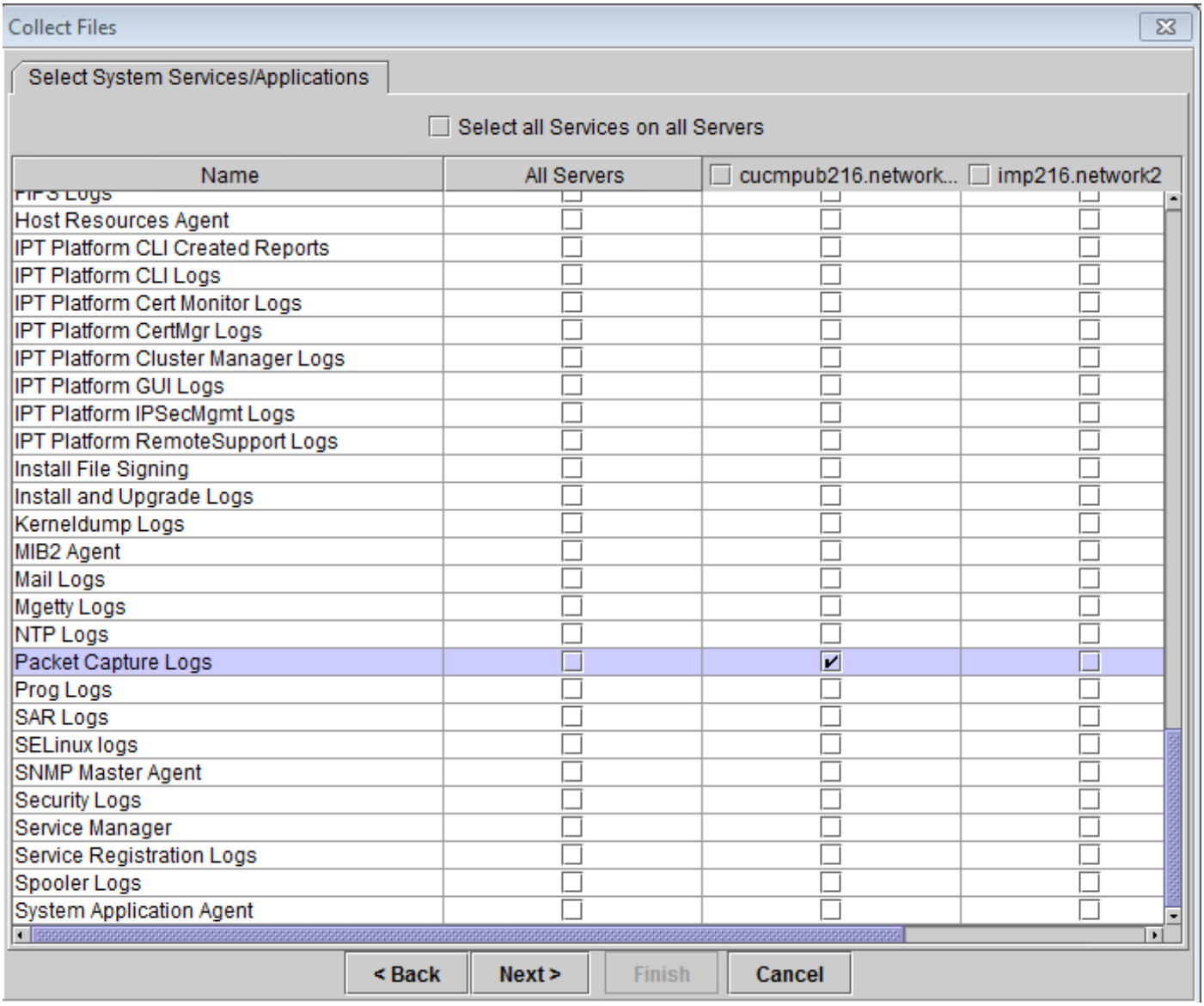
ステップ3:TLSハンドシェイク完了後にCUCM PCAPを停止する

図に示**すように、Control-C**を押してパケットキャプチャを停止します

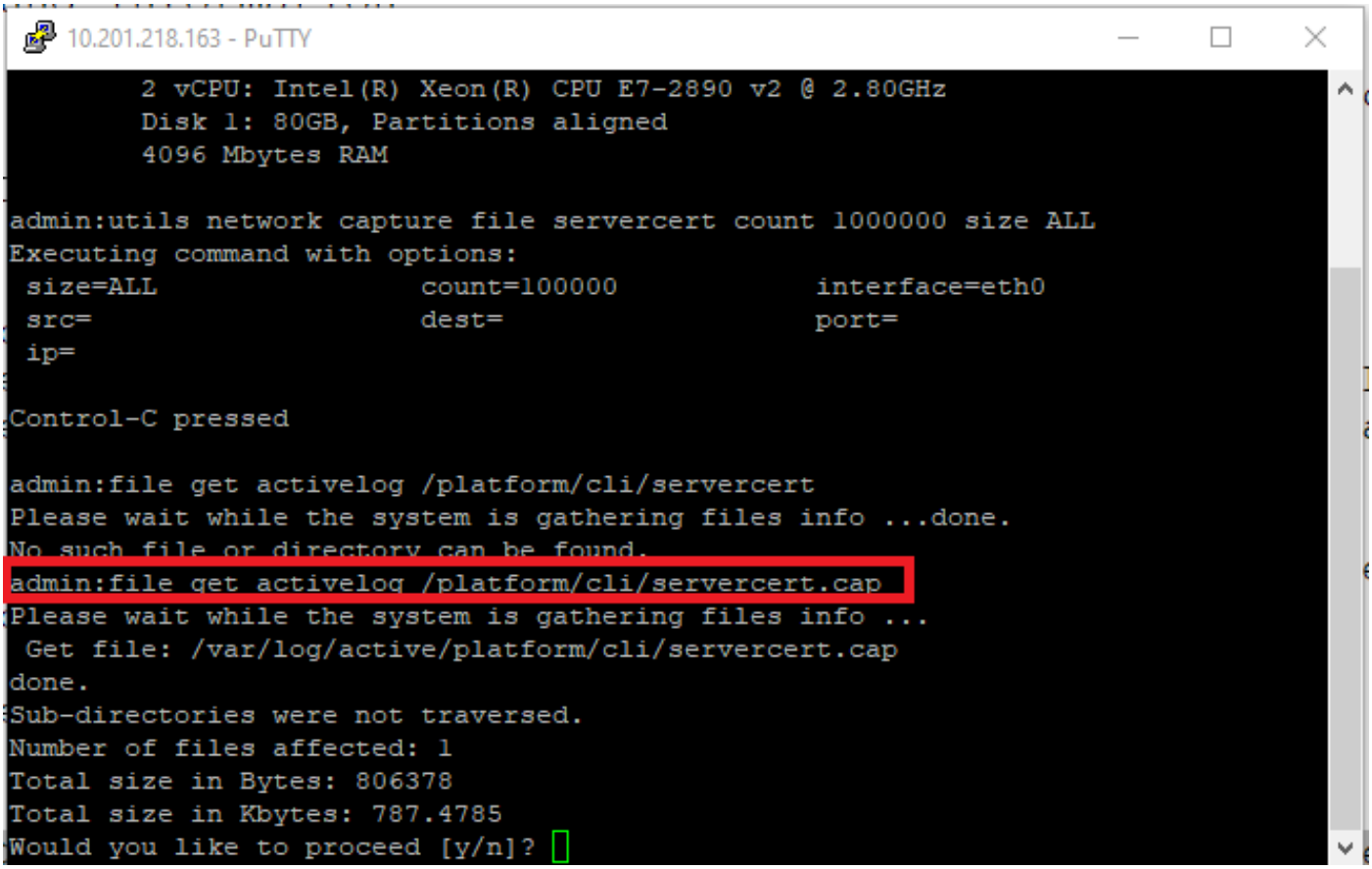


ステップ4：次の2つの方法のいずれかでパッカーキャプチャファイルをダウンロードします

1. CUCMノードのRTMTを起動し、**[System] > [Tools] > [Trace] > [Trace & Log Central] > [Collect Files]に移動し、[Packet Capture Logs]ボックスをオンにします**（pcapをダウンロードするにはRTMTプロセスをします）。

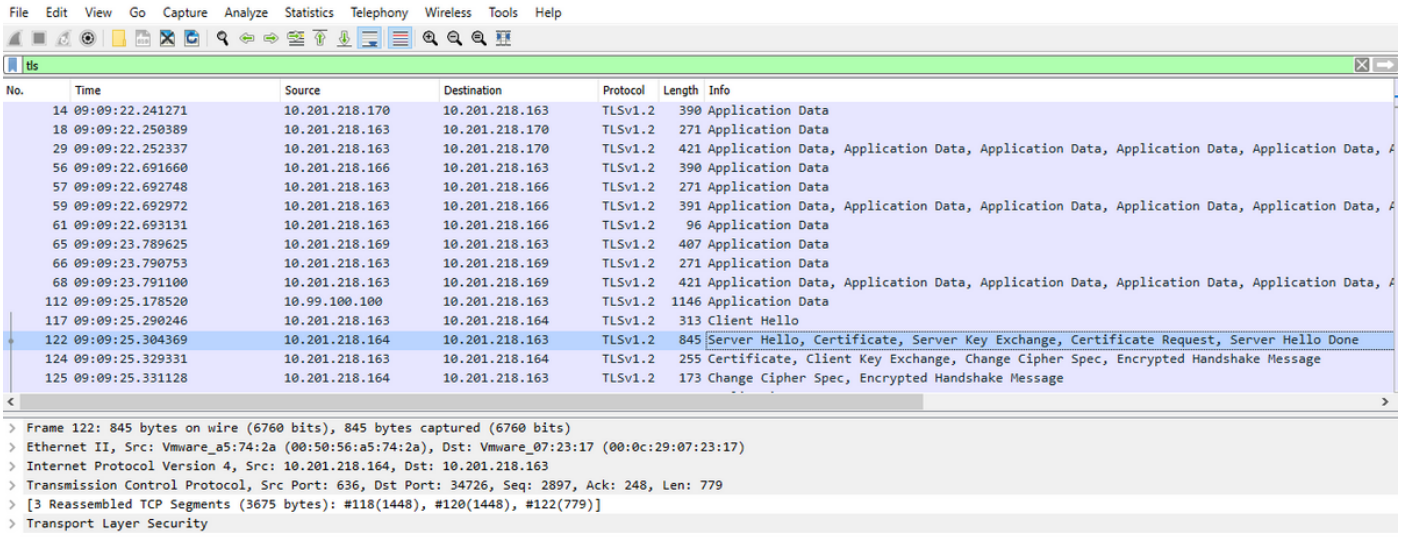


2. SFTP (Secure File Transport Protocol)サーバを起動し、CUCM SSHセッションで**file get activelog /patform/cli/<pcap filename>.capコマンドを実行します(プロンプトに従ってSFTPサーバにPCAPをダウンロードします**)。

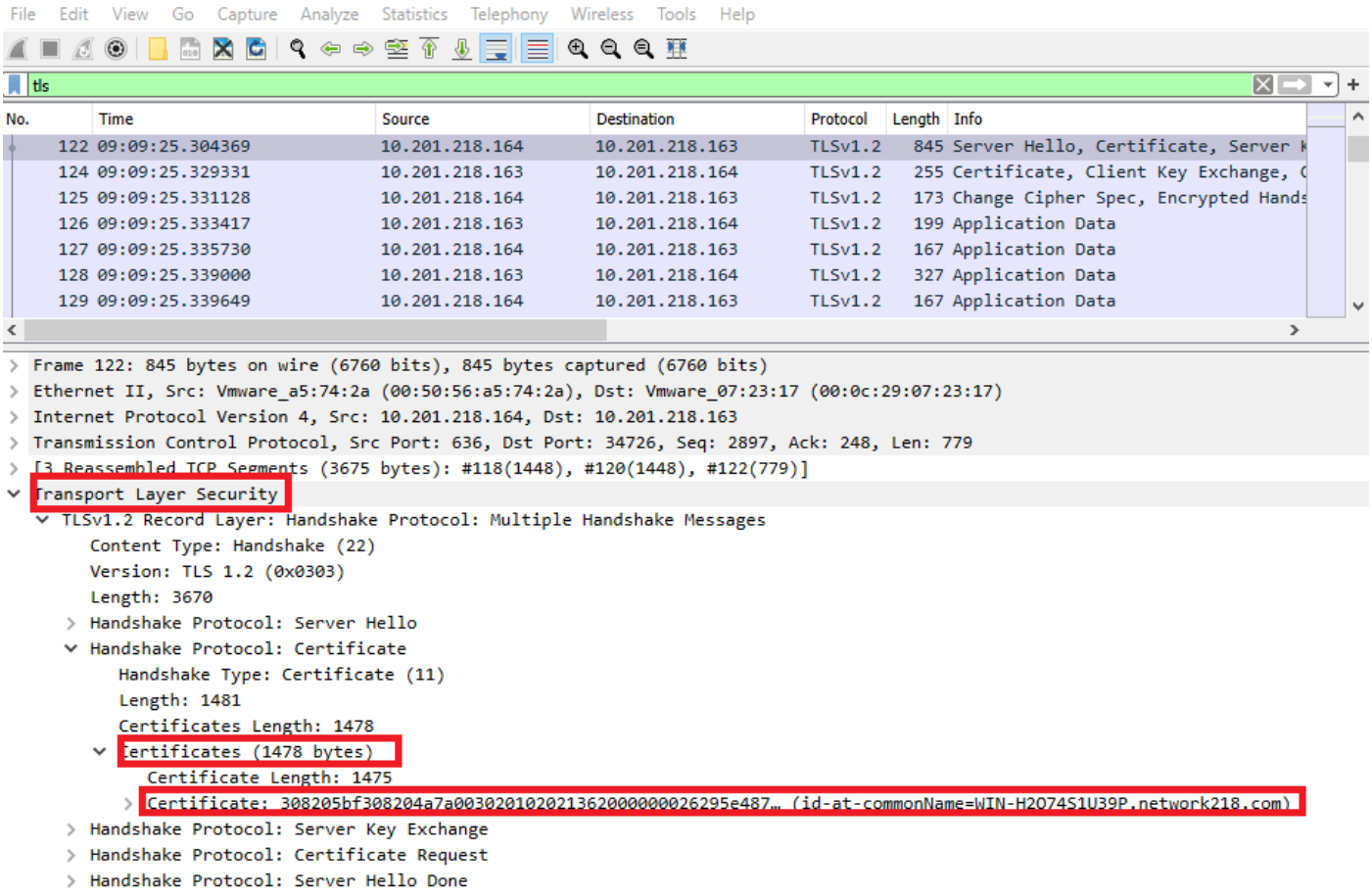


ステップ5：サーバがCUCMに提示する証明書の数を決定する

Wiresharkアプリケーションを使用してpcapを開き、**tlsでフィルタを実行**し、CUCMに提示されるサーバ証明書/証明書チェーンを含む**Server Hello**パケットを判別します。これは、図に示すように、フレーム122です。

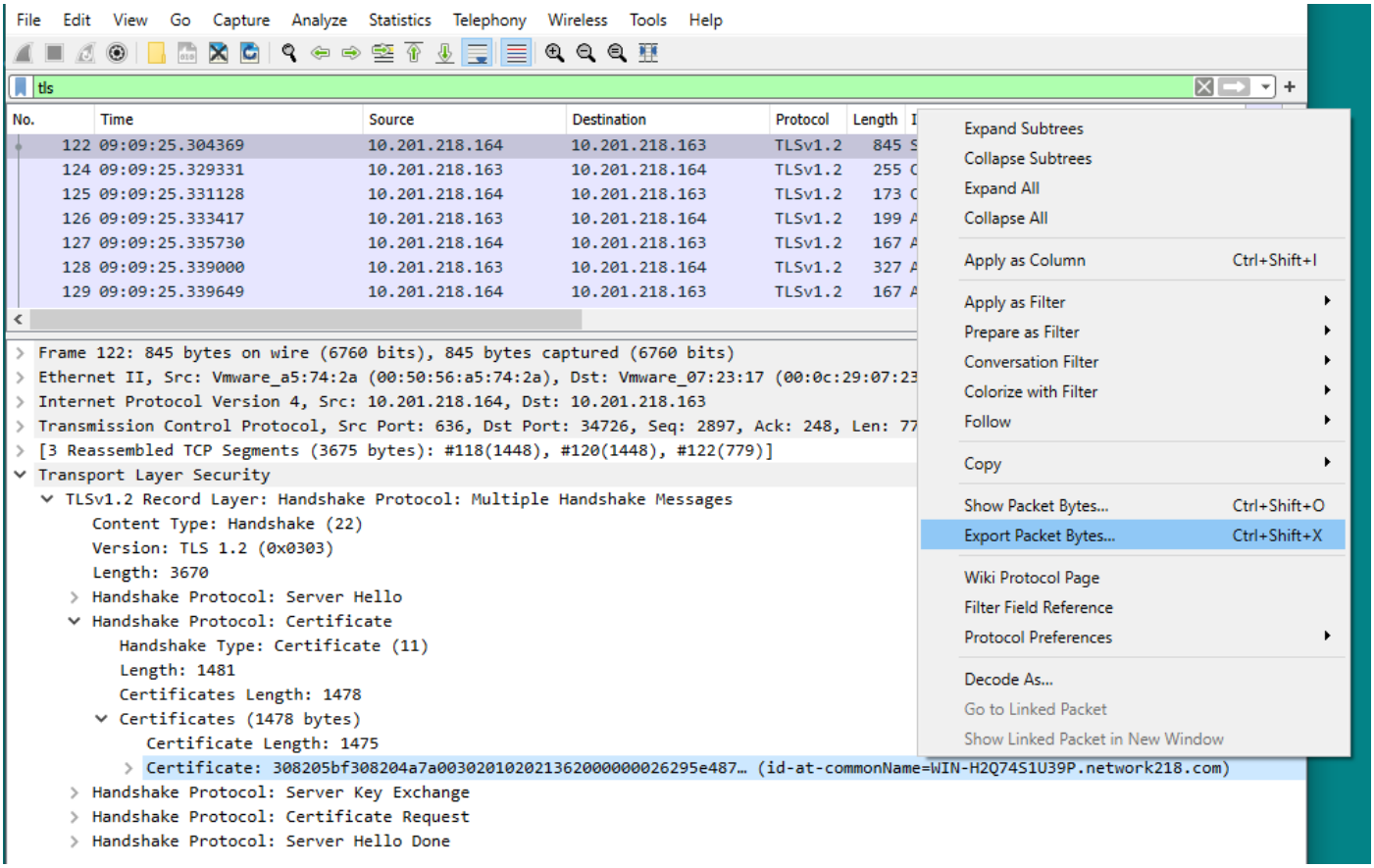


・ CUCMに提示される証明書の数を確認するには、証明書を含むServer Helloパケットから**[Transport Layer Security] > [Certificate]**の情報を展開します。一番上の証明書はサーバ証明書です。この場合、サーバ証明書である1つの証明書だけが図のように表示されます。

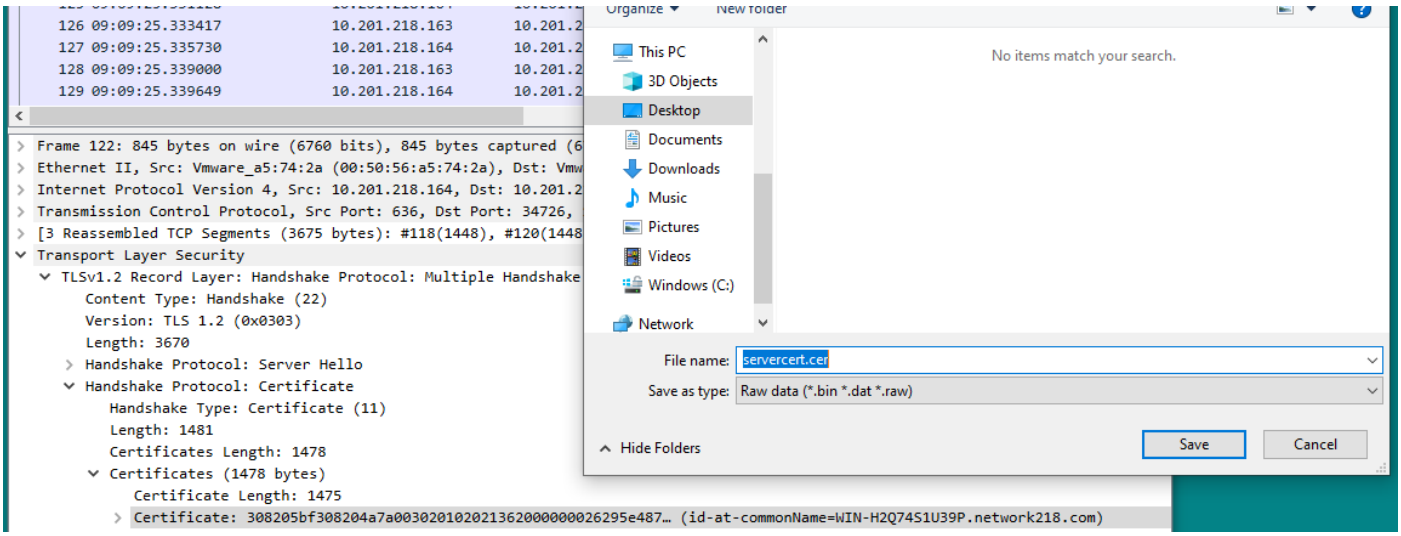


ステップ6:CUCM PCAPからサーバ証明書/証明書チェーンをエクスポートします

この例では、サーバ証明書だけが示されているため、サーバ証明書を調べる必要があります。図に示すように、サーバ証明書を右クリックし、[Export Packet Bytes]を選択して.cer証明書として保存します。

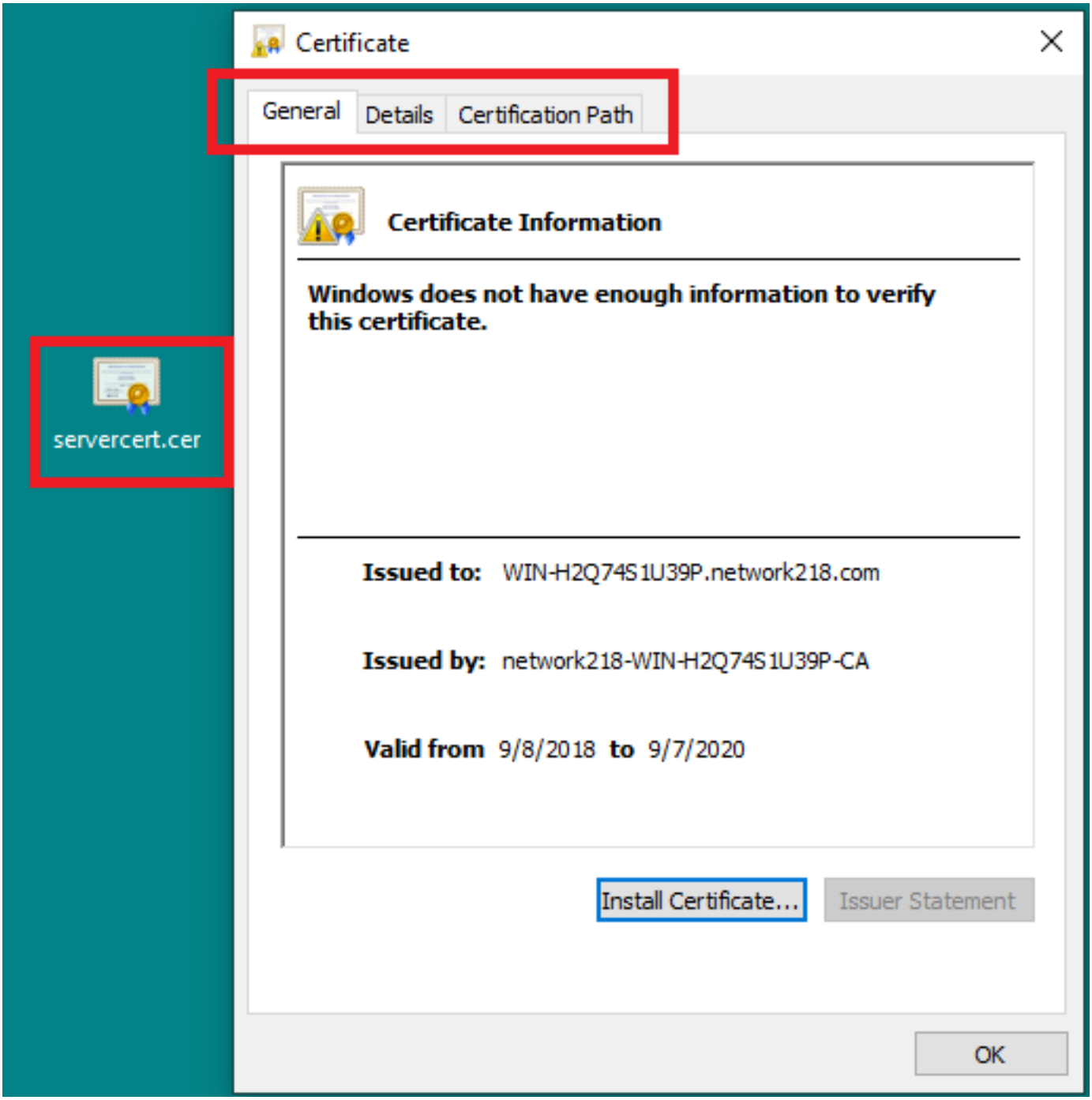


・後続のウィンドウで、.cerファイル名を入力し、[保存]をクリックします。次の図に示すように、デスクトップに保存されたファイルの名前はservercert.cerです（この場合はデスクトップに保存されます）。



ステップ7：保存した.CERファイルを開いて内容を確認する

.cerファイルをダブルクリックして、[General]、[Details]、および[Certificate Path]タブの情報を確認します（図を参照）。



確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。