PCAP(CUCM Packet Capture)에서 TLS 인증서를 내보내는 방법

목차

소개

이 문서에서는 Cisco CUCM(Unified Communications Manager) PCAP에서 인증서를 내보내는 절차에 대해 설명합니다.

기고자: Cisco TAC 엔지니어 Adrian Esquillo

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.
·TLS(Transport Layer Security) 핸드셰이크
·CUCM 인증서 관리
·SFTP(Secure File Transport Protocol) 서버
·실시간 모니터링 툴(RTMT)

·Wireshark 애플리케이션

사용되는 구성 요소

·CUCM 릴리스 9.X 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

서버에서 제공하는 서버 인증서/인증서 체인이 업로드할 인증서와 일치하는지 또는 CUCM Certificate Management에 업로드된 인증서와 일치하는지 확인하기 위해 서버 인증서/인증서 체인

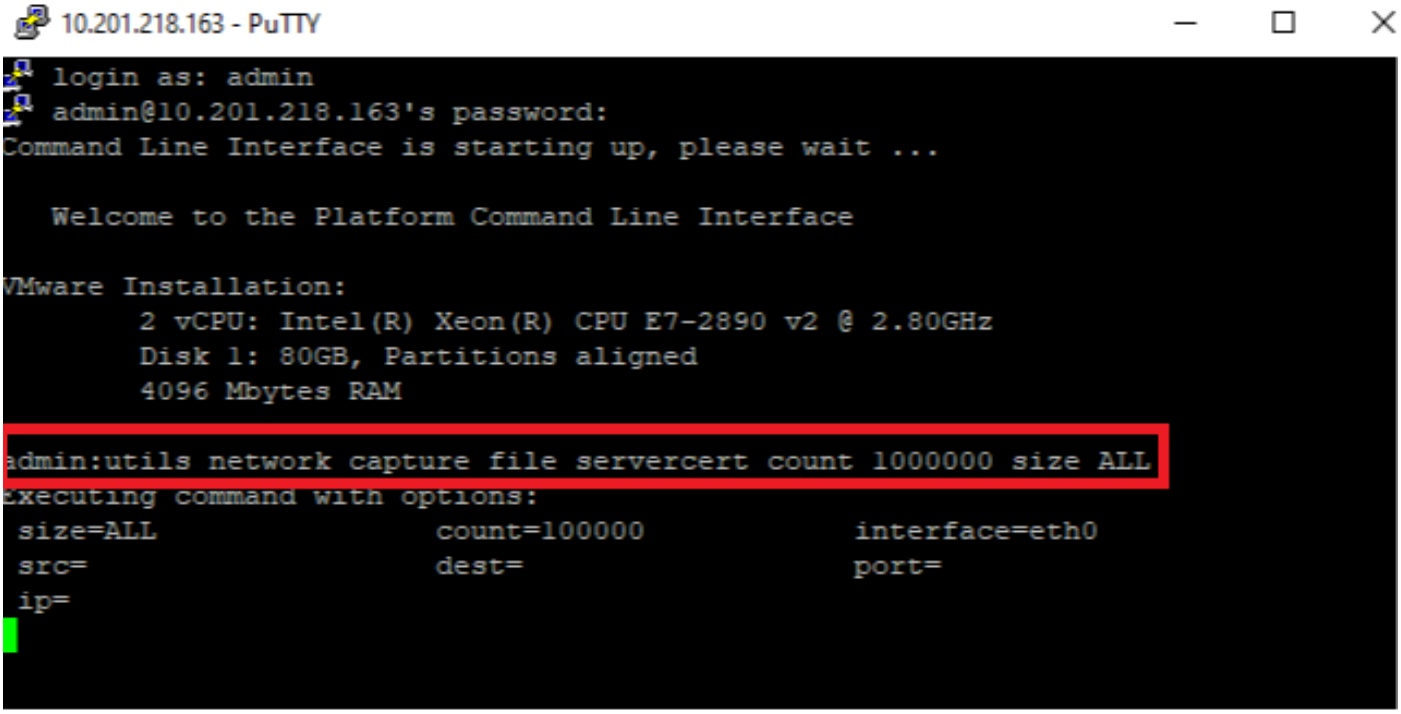
을 내보낼 수 있습니다.

TLS 핸드셰이크의 일부로서 서버는 CUCM에 서버 인증서/인증서 체인을 제공합니다.

CUCM PCAP에서 TLS 인증서 내보내기

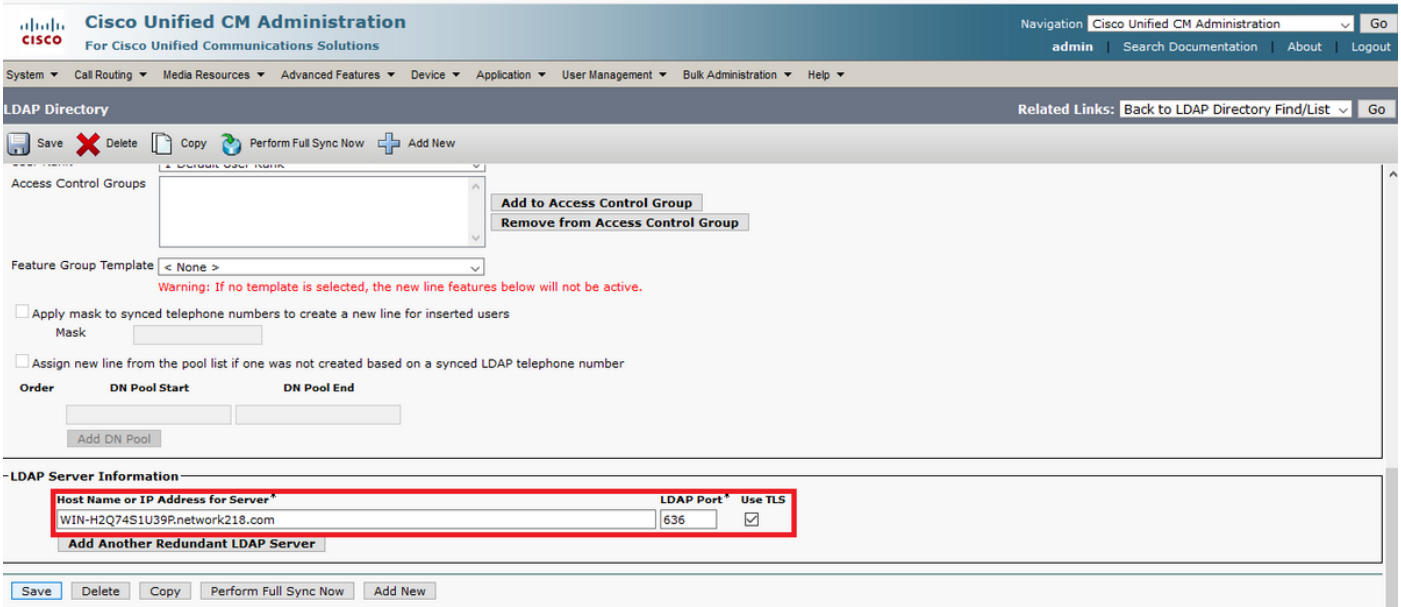
1단계. CUCM에서 packet capture 명령을 시작합니다.

CUCM 노드에 대한 SSH(Secure Shell) 연결을 설정하고 이미지에 표시된 대로 **utils network capture(또는 capture-rotate) 파일 <filename> count 10000000 size ALL**을 실행합니다.



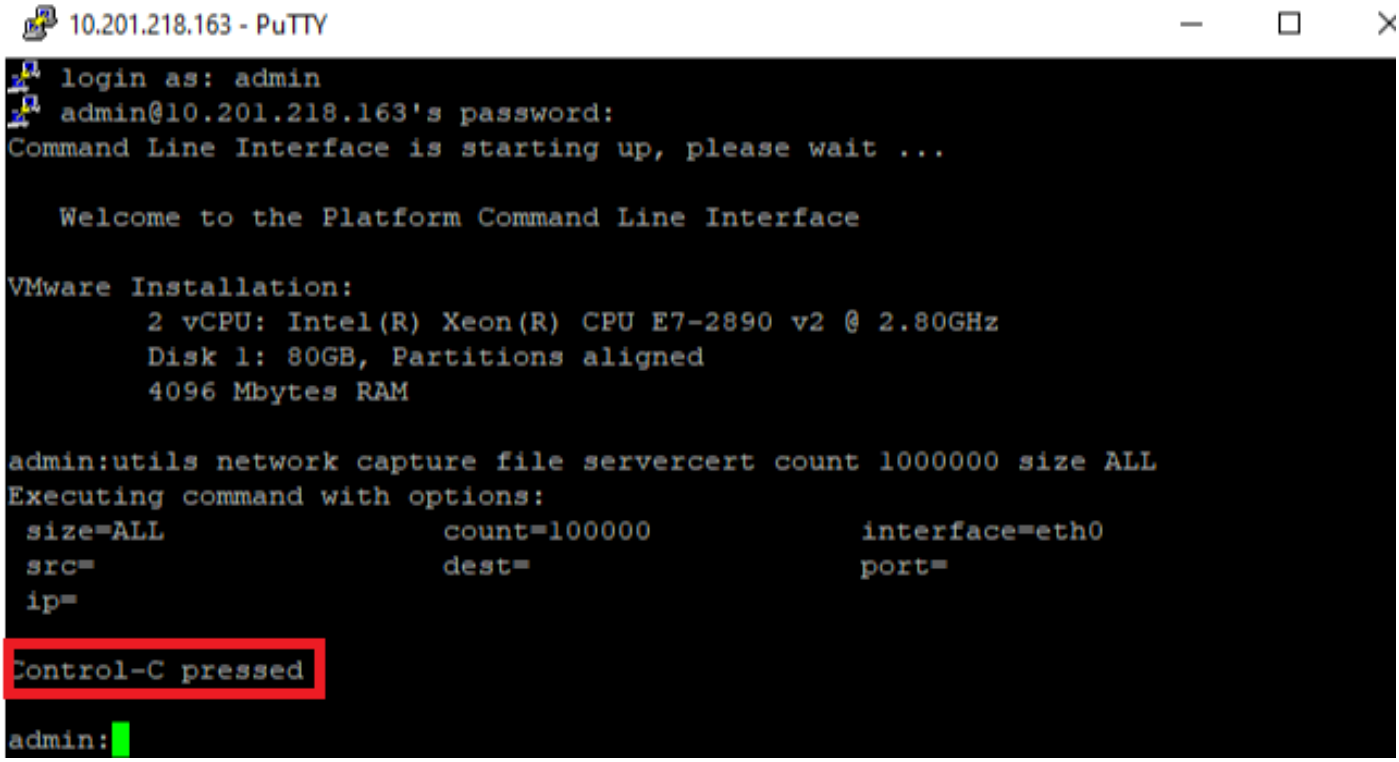
2단계. 서버와 CUCM 간의 TLS 연결을 시작합니다.

이 예에서는 이미지에 표시된 것처럼 TLS 포트 636에서 연결을 설정하여 LDAPS(Secure Lightweight Directory Access Protocol) 서버와 CUCM 간의 TLS 연결을 시작합니다.



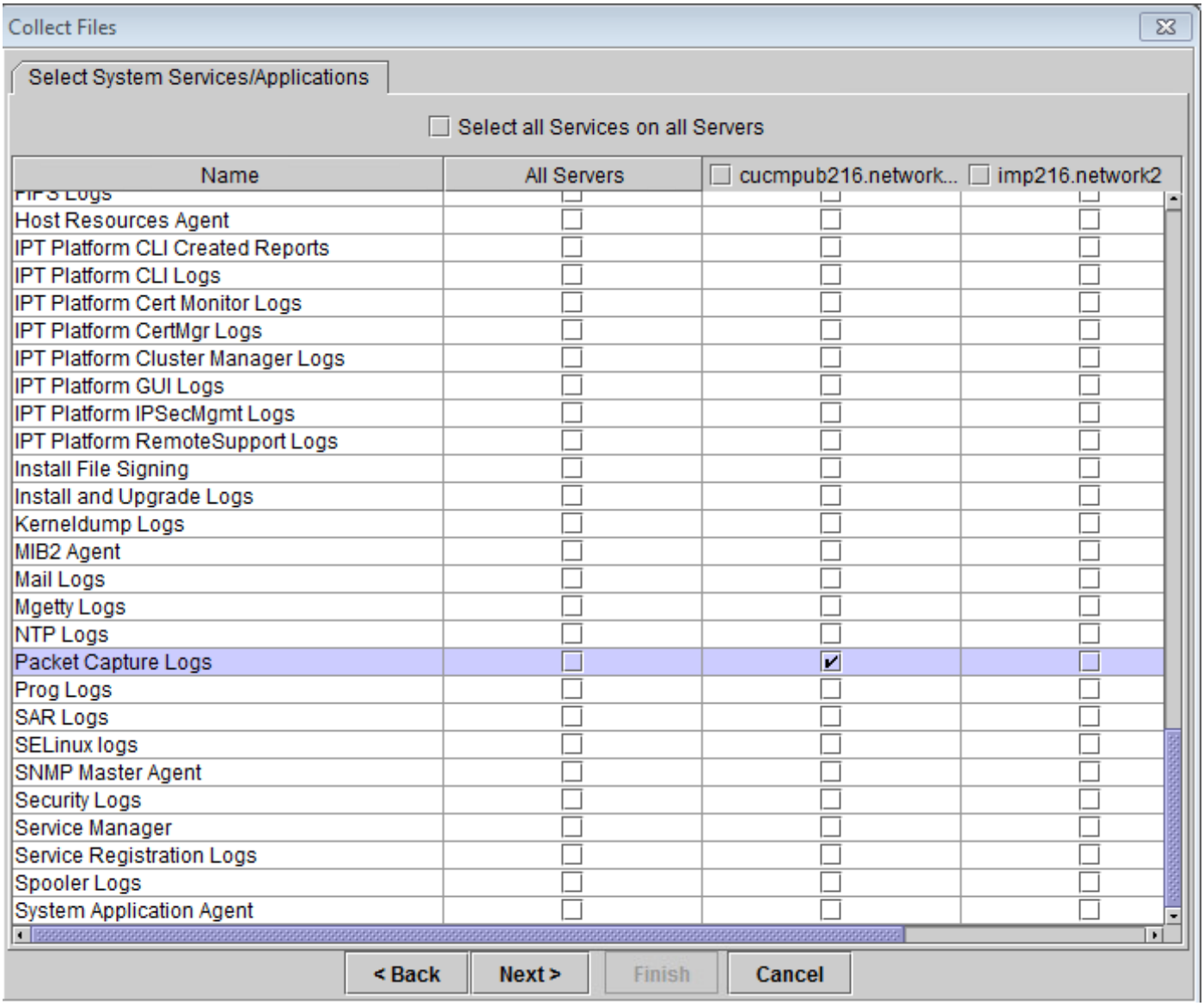
3단계. TLS 핸드셰이크가 완료된 후 CUCM PCAP를 중지합니다.

이미지에 표시된 대로 패킷 캡처를 중지하려면 Control-C를 누릅니다.

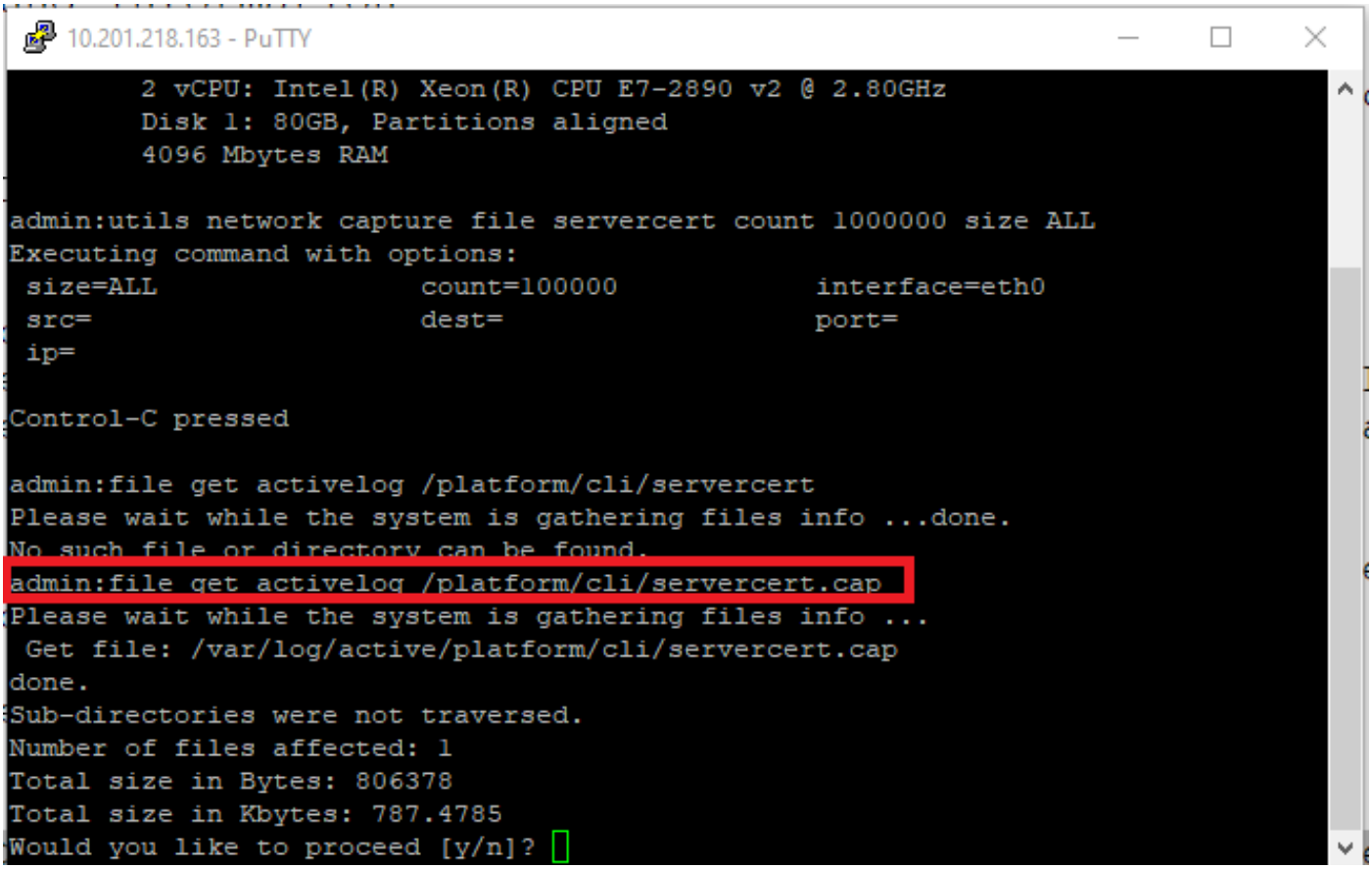


4단계. 나열된 두 가지 방법 중 하나로 패키지 캡처 파일을 다운로드합니다.

1. CUCM 노드에 대해 RTMT를 시작하고 **System > Tools > Trace > Trace & Log Central > Collect Files로** 이동하고 **Packet Capture Logs** 상자(pcap을 다운로드하려면 RTMT 프로세스를 계속 진행)를 선택합니다.

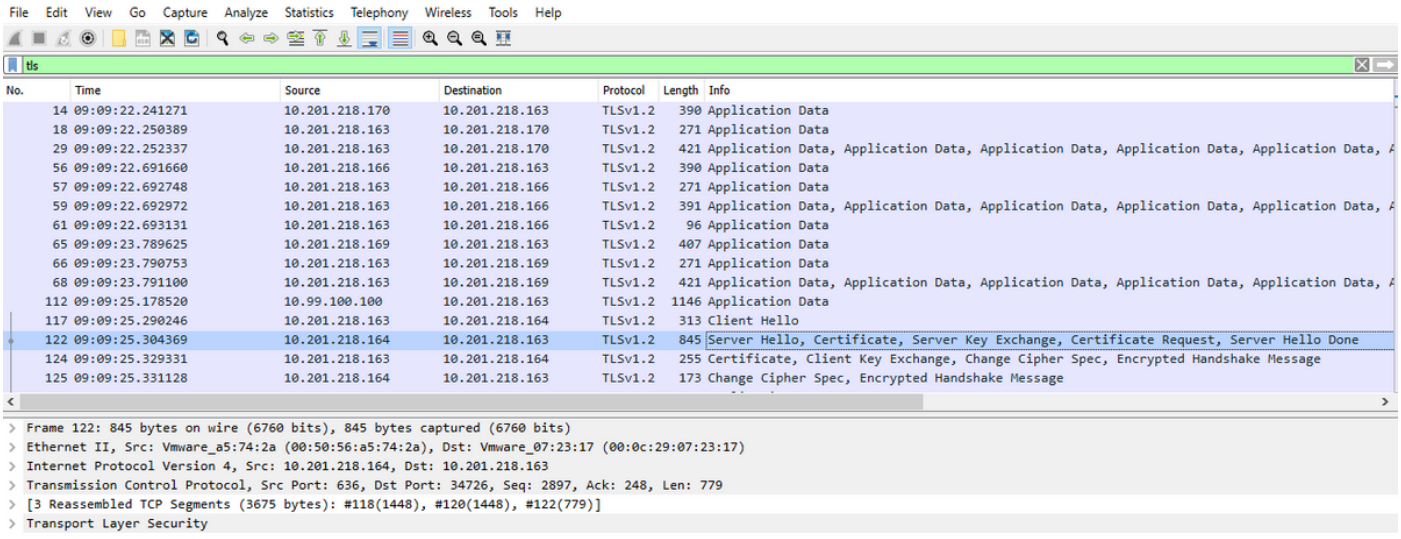


2. SFTP(Secure File Transport Protocol) 서버를 시작하고 CUCM SSH 세션에서 이미지에 표시된 대로 명령 **파일 get activelog /patform/cli/<pcap filename>.cap**(SFTP 서버의 PCAP를 다운로드하려면 프롬프트를 계속 진행)

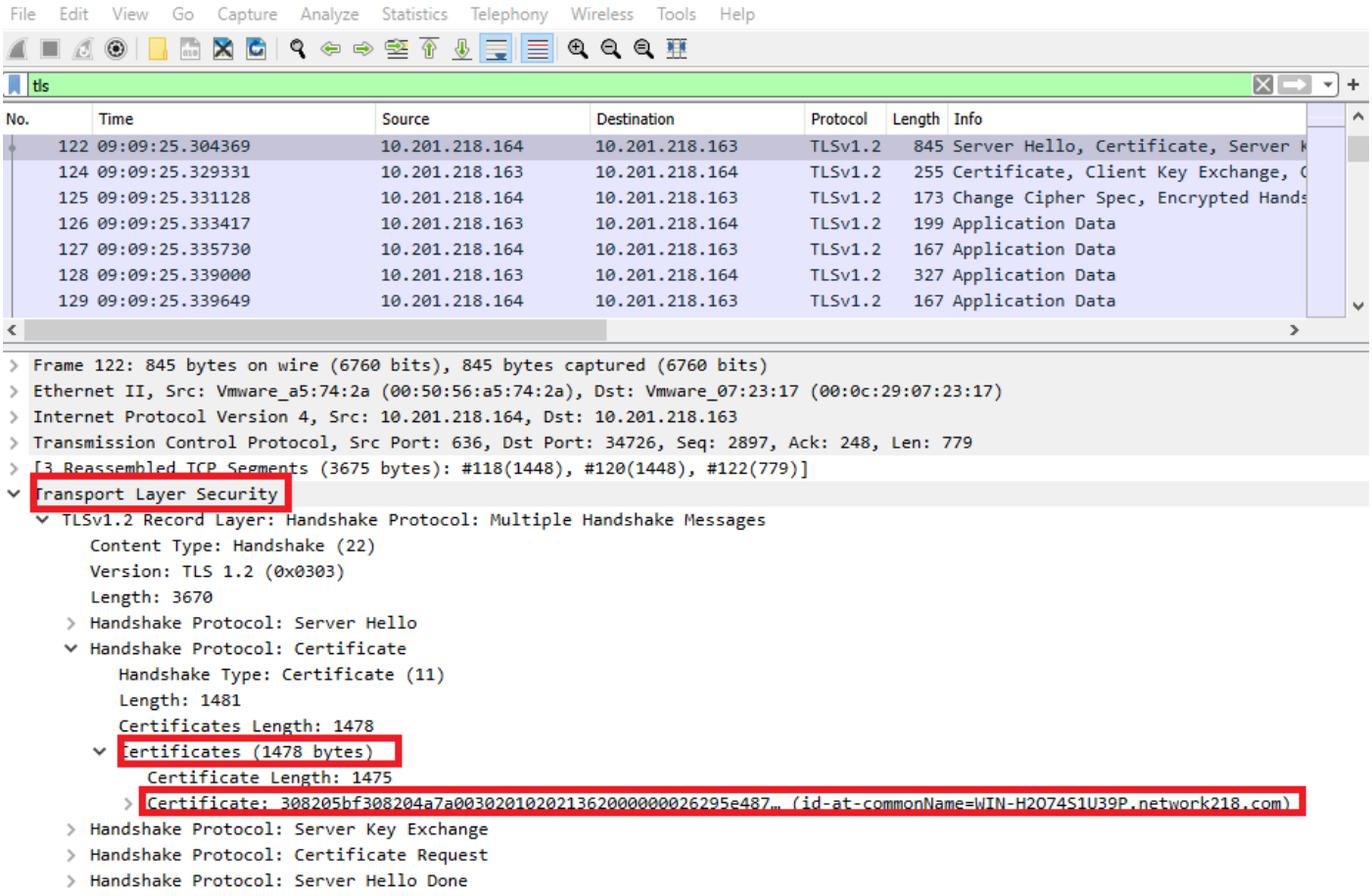


5단계. 서버에서 CUCM에 제공한 인증서 수를 확인합니다.

Wireshark 애플리케이션을 사용하여 pcap을 열고 **tls**를 필터링하여 CUCM에 제공된 서버 인증서 /인증서 체인이 포함된 **Server Hello**로 패킷을 확인합니다.이것은 이미지에 표시된 프레임 122입니다.

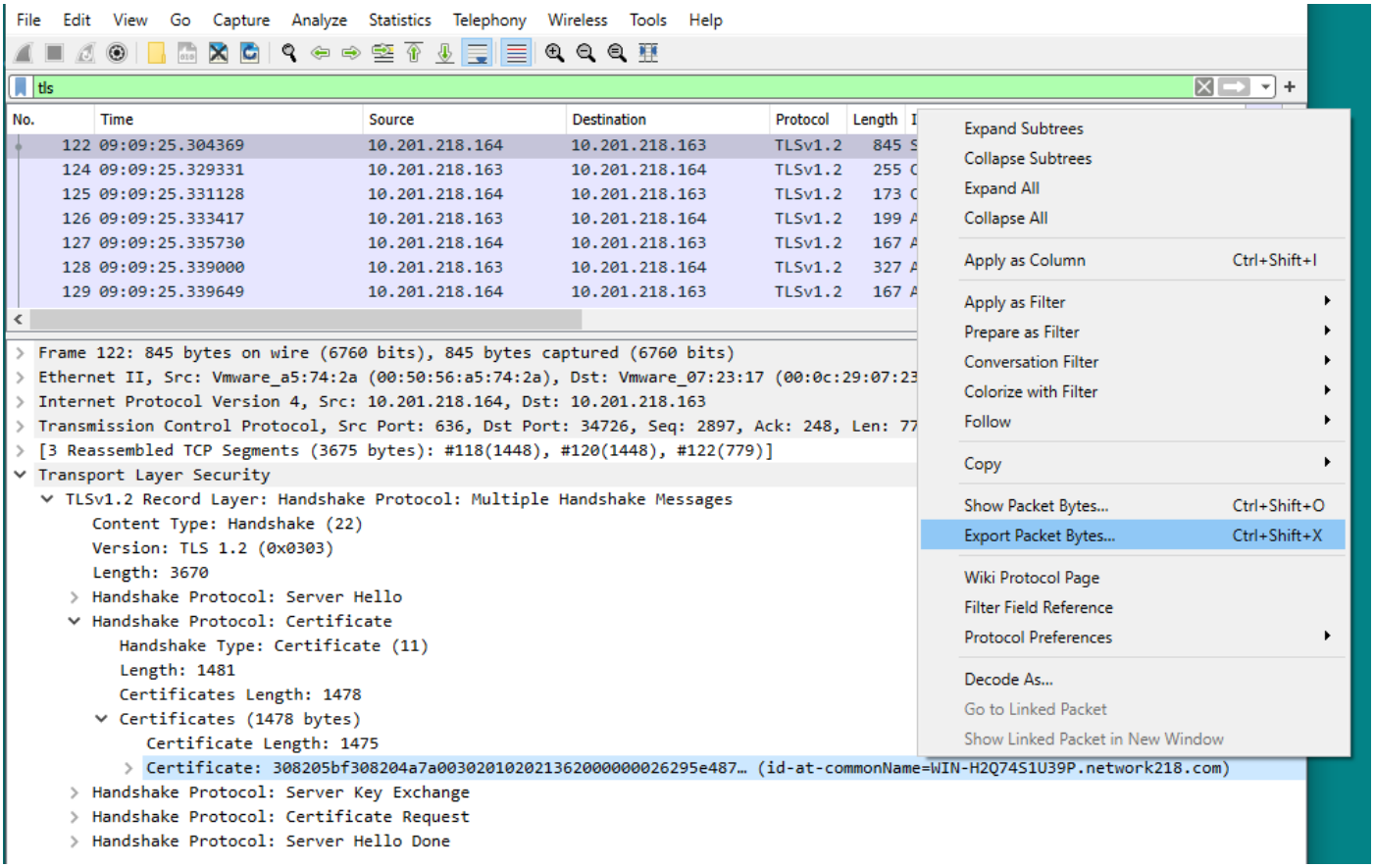


·CUCM에 표시되는 인증서 수를 확인하기 위해 Server Hello 패킷에서 Transport **Layer Security > Certificate** information을 확장합니다.상위 인증서는 서버 인증서입니다.이 경우 이미지에 표시된 것처럼 서버 인증서인 1개의 인증서만 표시됩니다.

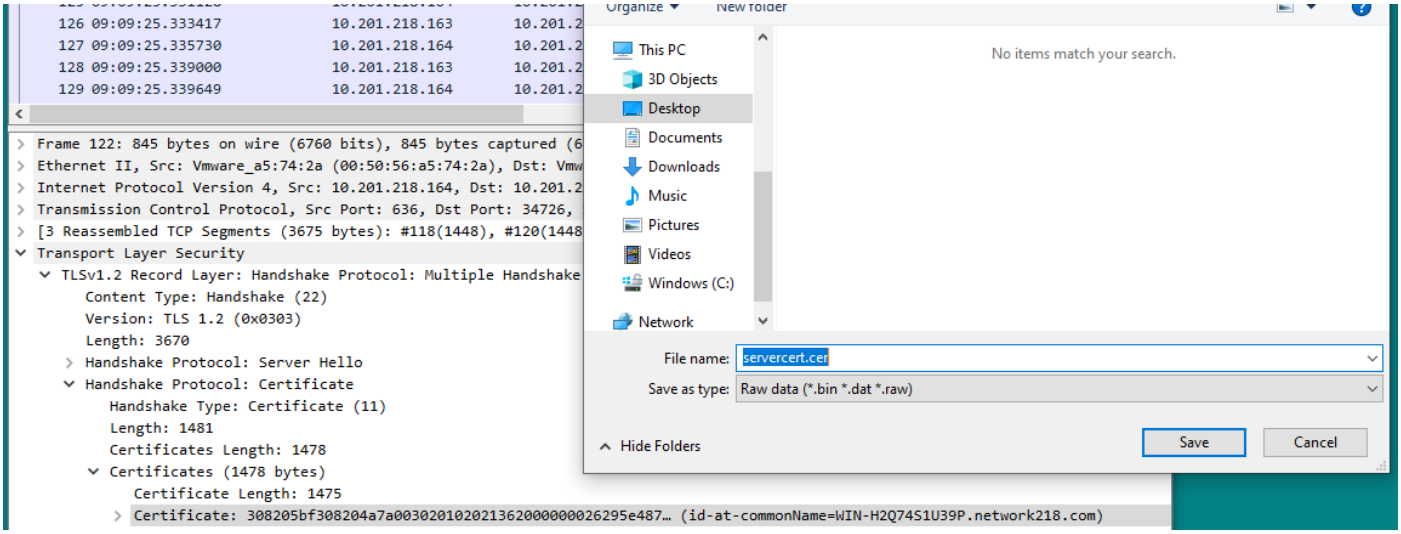


6단계. CUCM PCAP에서 서버 인증서/인증서 체인을 내보냅니다.

이 예에서는 서버 인증서만 표시되므로 서버 인증서를 검사해야 합니다.서버 인증서를 마우스 오른쪽 버튼으로 클릭하고 **Export Packet Bytes**를 선택하여 이미지에 표시된 것처럼 .cer 인증서로 저장합니다.

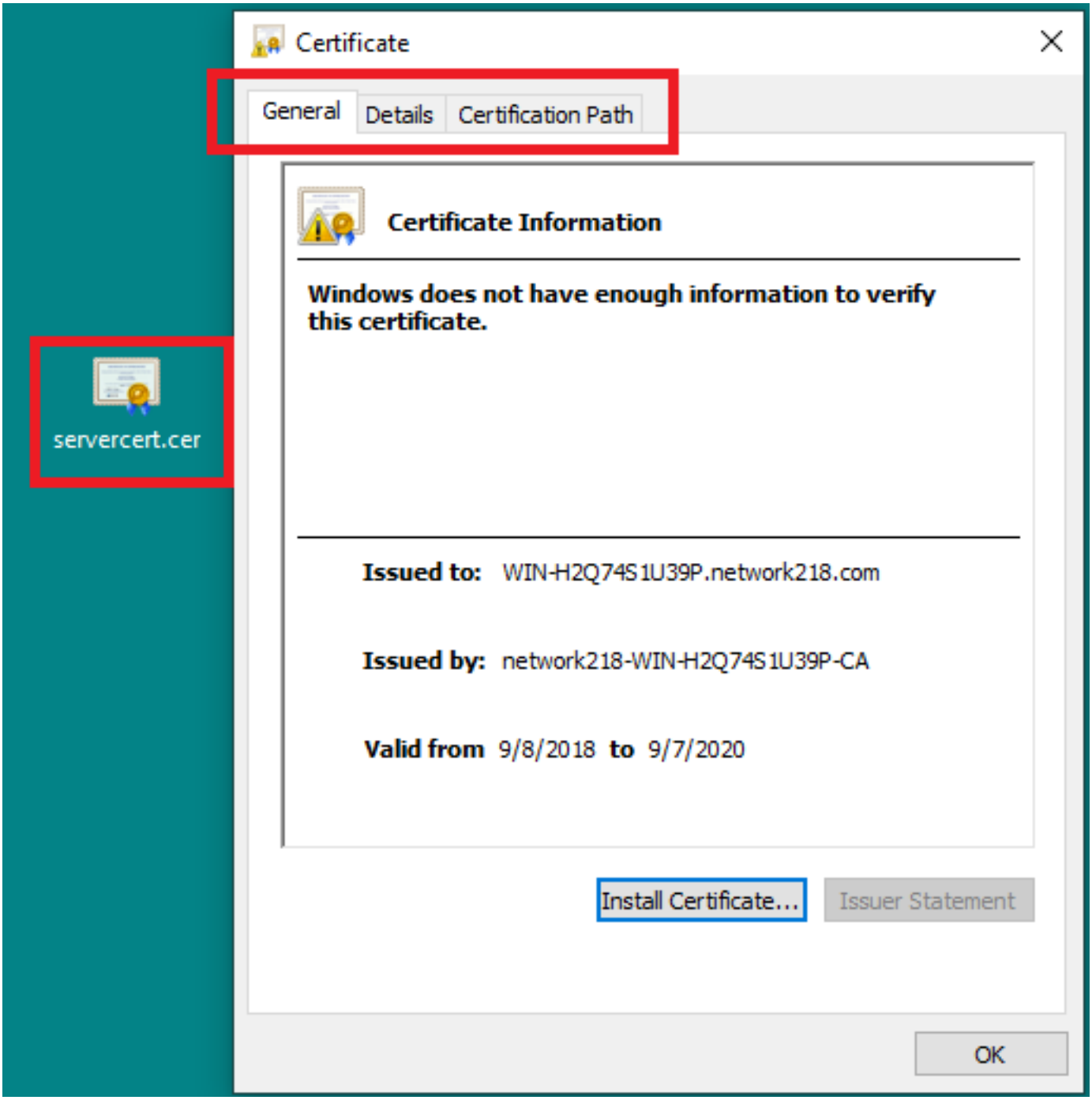


·후속 창에서 .cer 파일 이름을 입력한 다음 저장을 클릭합니다.다음 이미지에 표시된 대로 (이 경우 데스크톱에) 저장된 파일의 이름은 servercert.cer입니다.



7단계. 내용을 검사하기 위해 저장된 .CER 파일을 엽니다.

.cer 파일을 두 번 클릭하여 이미지에 표시된 대로 **General**, Details 및 **Certificate Path** 탭의 정보를 확인합니다.



다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.