How to Export TLS Certifcate from CUCM Packet Capture (PCAP)

Contents

Introduction

This document describes the procedure to export a certificate from a Cisco Unified Communications Manager (CUCM) PCAP.

Contributed by Adrian Esquillo, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:
- Transport Layer Security (TLS) Handshake
- CUCM Certificate Management
- Secure File Transport Protocol (SFTP) server
- Realtime Monitoring Tool (RTMT)

- Wireshark Application

Components Used

- CUCM release 9.X and higher

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

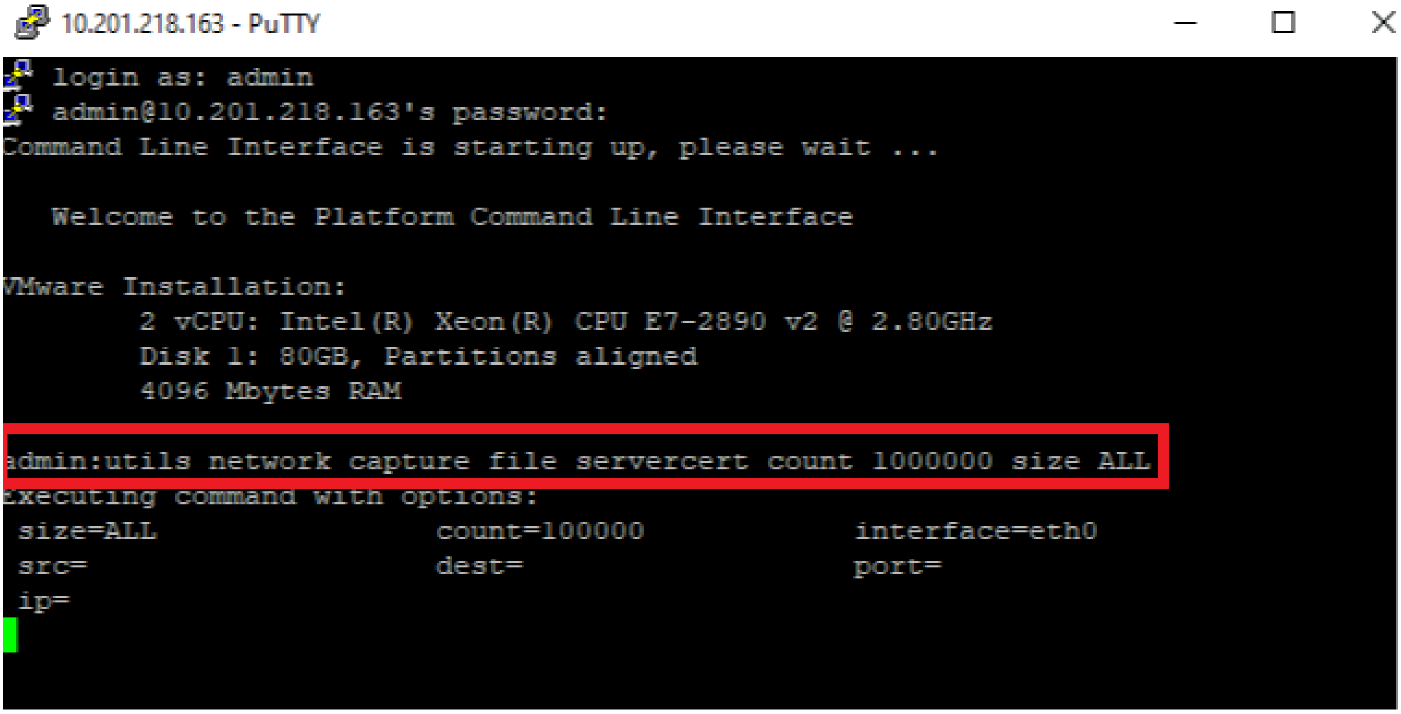
A server certificate/certificate chain can be exported in order to confirm that the server certificate/certificate chain provided by the server matches the certificate(s) to upload or that are uploaded to CUCM Certificate Management.

As part of the TLS handshake, the server provides its server certificate/certificate chain to CUCM.

Export TLS Certificate from CUCM PCAP

Step 1. Start the packet capture command on CUCM

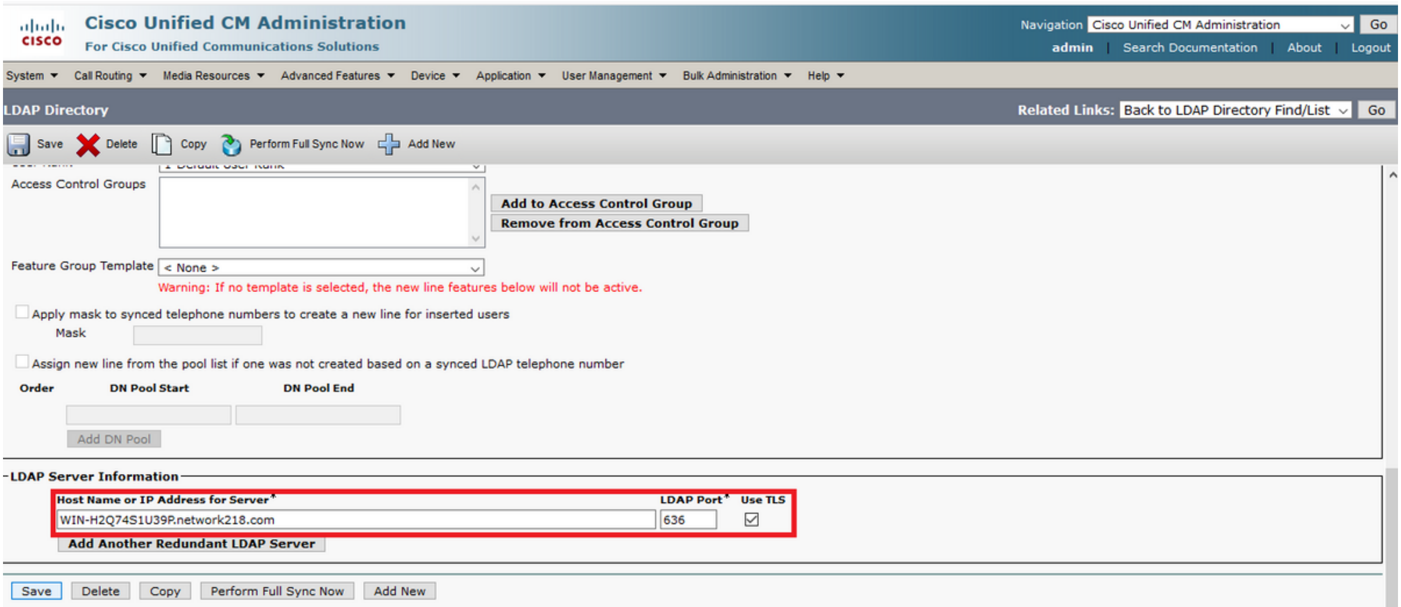
Establish a Secure Shell (SSH) connection to the CUCM node and run the command **utils network capture (or capture-rotate) file <filename> count 1000000 size ALL**, as shown in the image:



```
 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=
```

Step 2. Start a TLS connection between Server and CUCM

In this example, you start a TLS connection between a Secure Lightweight Directory Access Protocol (LDAPS) server and CUCM by establishes a connection on TLS port 636, as shown in the image:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
LDAP Directory
Related Links: Back to LDAP Directory Find/List Go
Save Delete Copy Perform Full Sync Now Add New
Add to Access Control Group
Remove from Access Control Group
Add DN Pool
Add Another Redundant LDAP Server
Save Delete Copy Perform Full Sync Now Add New

Access Control Groups

Feature Group Template < None >

Warning: If no template is selected, the new line features below will not be active.

□ Apply mask to synced telephone numbers to create a new line for inserted users

Mask

□ Assign new line from the pool list if one was not created based on a synced LDAP telephone number

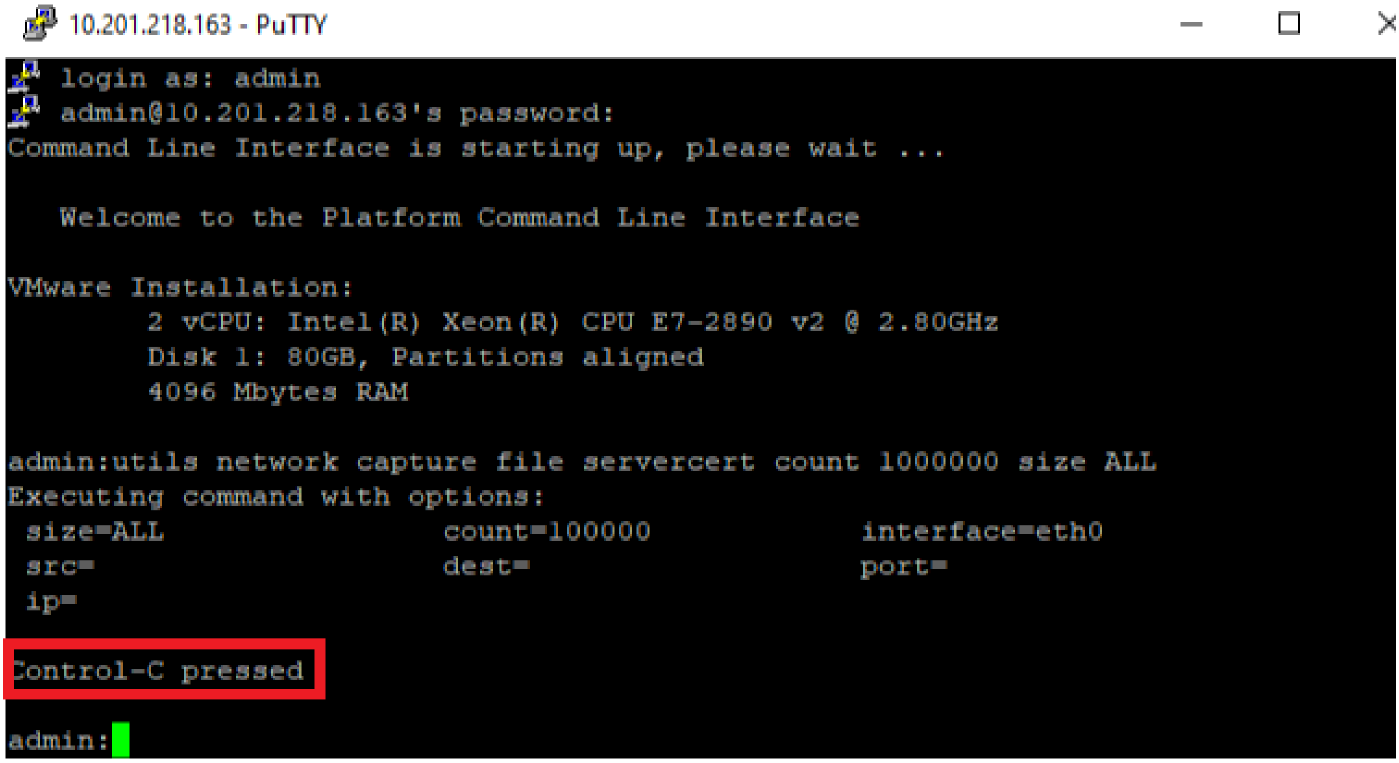
Order DN Pool Start DN Pool End

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
WIN-H2Q74S1U39P.network218.com	636	☑

Step 3. Stop CUCM PCAP after TLS handshake Is completed

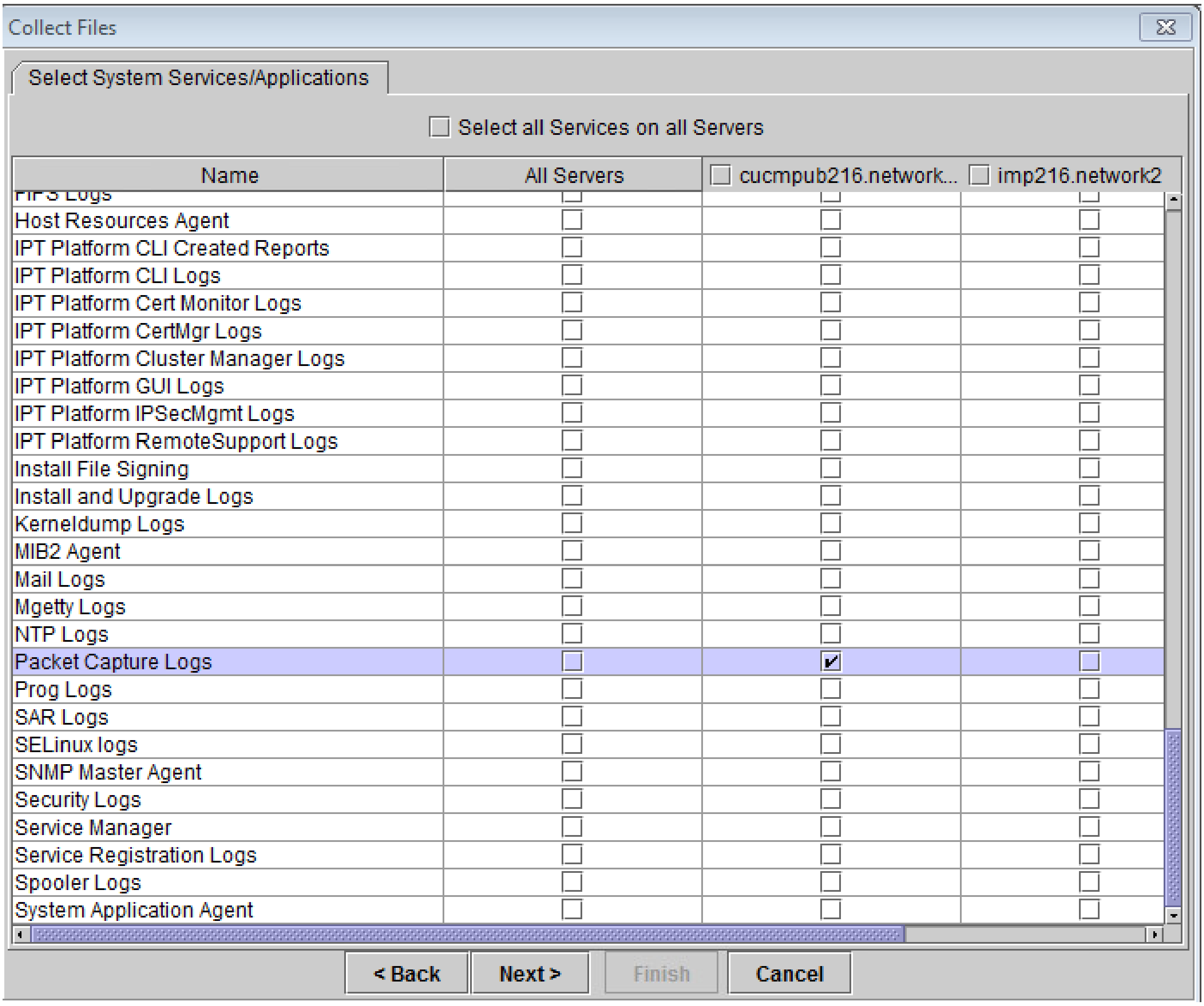
Press **Control-C** to stop the packet capture, as shown in the image



```
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=

Control-C pressed

admin:
```

Step 4. Download the packer capture file by any of the two methods listed

1. Launch RTMT for CUCM node and Navigate to **System > Tools > Trace > Trace & Log Central > Collect Files** and check the **Packet Capture Logs** box (continue through the RTMT process in order to download the pcap), as shown in the image:

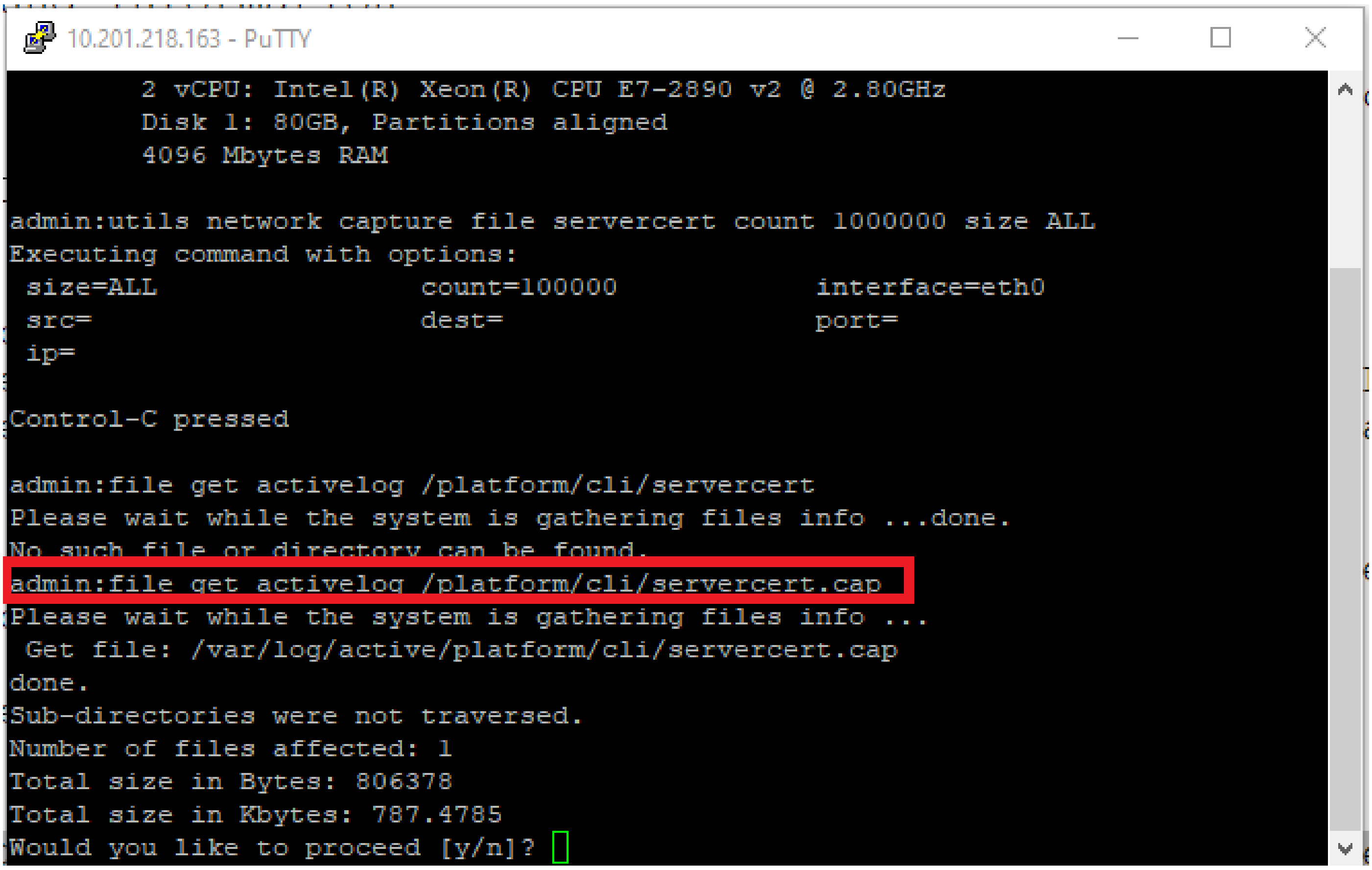


Select System Services/Applications

□ Select all Services on all Servers

Name	All Servers	□ cucmpub216.network...	□ imp216.network2
FIPS Logs	□	□	□
Host Resources Agent	□	□	□
IPT Platform CLI Created Reports	□	□	□
IPT Platform CLI Logs	□	□	□
IPT Platform Cert Monitor Logs	□	□	□
IPT Platform CertMgr Logs	□	□	□
IPT Platform Cluster Manager Logs	□	□	□
IPT Platform GUI Logs	□	□	□
IPT Platform IPSecMgmt Logs	□	□	□
IPT Platform RemoteSupport Logs	□	□	□
Install File Signing	□	□	□
Install and Upgrade Logs	□	□	□
Kerneldump Logs	□	□	□
MIB2 Agent	□	□	□
Mail Logs	□	□	□
Mgetty Logs	□	□	□
NTP Logs	□	□	□
Packet Capture Logs	□	☑	□
Prog Logs	□	□	□
SAR Logs	□	□	□
SELinux logs	□	□	□
SNMP Master Agent	□	□	□
Security Logs	□	□	□
Service Manager	□	□	□
Service Registration Logs	□	□	□
Spooler Logs	□	□	□
System Application Agent	□	□	□

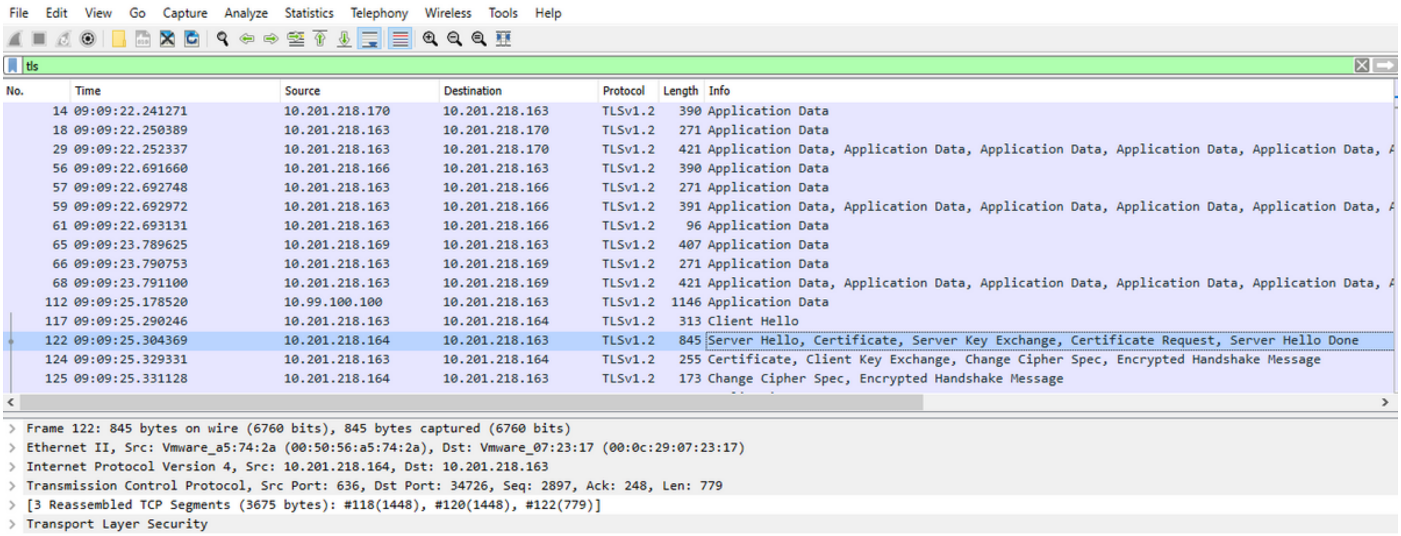
2. Start a Secure File Transport Protocol (SFTP) server and in the CUCM SSH session run the command **file get activelog /patform/cli/<pcap filename>.cap** (continue through the prompts in order to download the PCAP on SFTP server), as shown in the image:



```
        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]?
```

Step 5. Determine the Number of Certificates Presented to CUCM by the Server

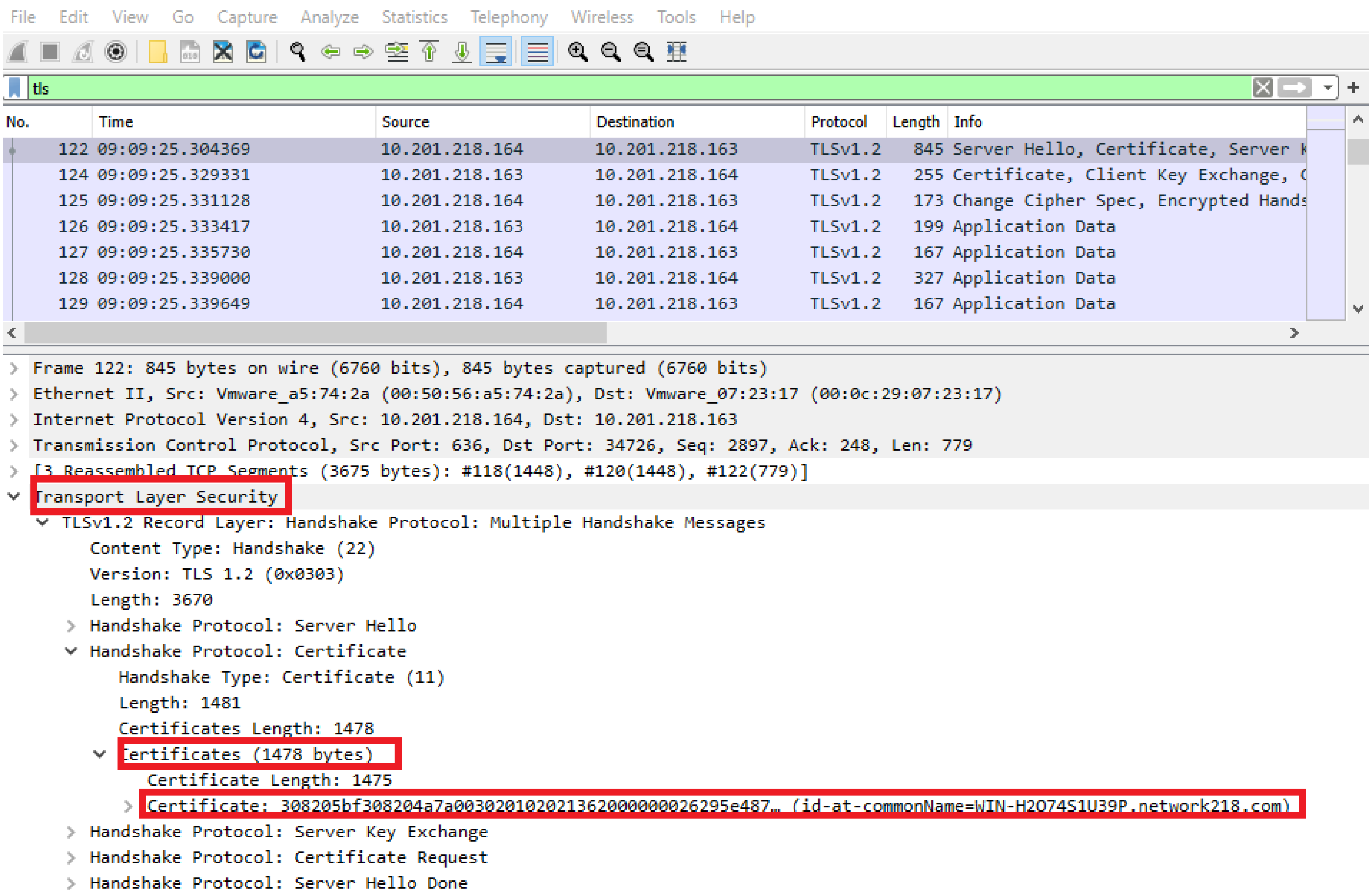
Utilize Wireshark application in order to open the pcap and filter on **tls** to determine the packet with **Server Hello** that contains the server certificate/certificate chain presented to CUCM. This is frame 122, as shown in the image:



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tls
No.  Time             Source          Destination     Protocol Length Info
 14 09:09:22.241271  10.201.218.170  10.201.218.163  TLSv1.2   390 Application Data
 18 09:09:22.250389  10.201.218.163  10.201.218.170  TLSv1.2   271 Application Data
 29 09:09:22.252337  10.201.218.163  10.201.218.170  TLSv1.2   421 Application Data, Application Data, Application Data, Application Data, Application Data, A
 56 09:09:22.691660  10.201.218.166  10.201.218.163  TLSv1.2   390 Application Data
 57 09:09:22.692748  10.201.218.163  10.201.218.166  TLSv1.2   271 Application Data
 59 09:09:22.692972  10.201.218.163  10.201.218.166  TLSv1.2   391 Application Data, Application Data, Application Data, Application Data, Application Data, A
 61 09:09:22.693131  10.201.218.163  10.201.218.166  TLSv1.2    96 Application Data
 65 09:09:23.789625  10.201.218.169  10.201.218.163  TLSv1.2   407 Application Data
 66 09:09:23.790753  10.201.218.163  10.201.218.169  TLSv1.2   271 Application Data
 68 09:09:23.791100  10.201.218.163  10.201.218.169  TLSv1.2   421 Application Data, Application Data, Application Data, Application Data, Application Data, A
112 09:09:25.178520  10.99.100.100   10.201.218.163  TLSv1.2  1146 Application Data
117 09:09:25.290246  10.201.218.163  10.201.218.164  TLSv1.2   313 Client Hello
122 09:09:25.304369  10.201.218.164  10.201.218.163  TLSv1.2   845 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
124 09:09:25.329331  10.201.218.163  10.201.218.164  TLSv1.2   255 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
125 09:09:25.331128  10.201.218.164  10.201.218.163  TLSv1.2   173 Change Cipher Spec, Encrypted Handshake Message

> 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
```

- Expand the **Transport Layer Security > Certificate** information from the Server Hello packet with certificate in order to determine the number of certificates presented to CUCM. The top certificate is the server certificate. In this case only 1 certificate, the server certificate, is presented as shown in the image:

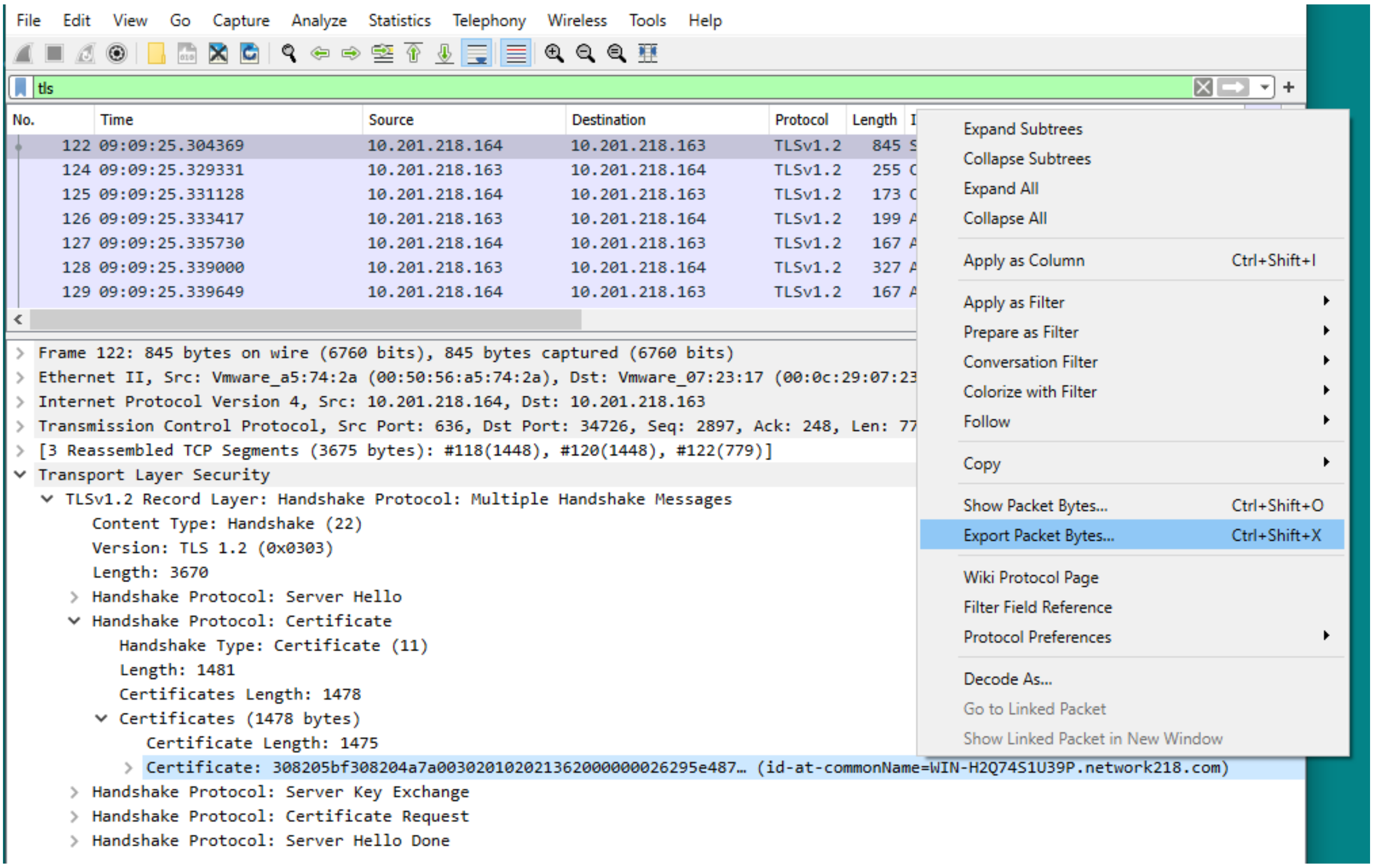

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
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)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3670
    > Handshake Protocol: Server Hello
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1481
        Certificates Length: 1478
      v Certificates (1478 bytes)
          Certificate Length: 1475
        > Certificate: 308205bf308204a7a00302010202136200000026295e487… (id-at-commonName=WIN-H2O74S1U39P.network218.com)
    > Handshake Protocol: Server Key Exchange
    > Handshake Protocol: Certificate Request
    > Handshake Protocol: Server Hello Done
```

Step 6. Export the server certificate/certificate chain from the CUCM PCAP

In this example, only the server certificate is presented, so you need to examine the server certificate. Right click on the server certificate and select **Export Packet Bytes** in order to save as a .cer certificate, as shown in the image:

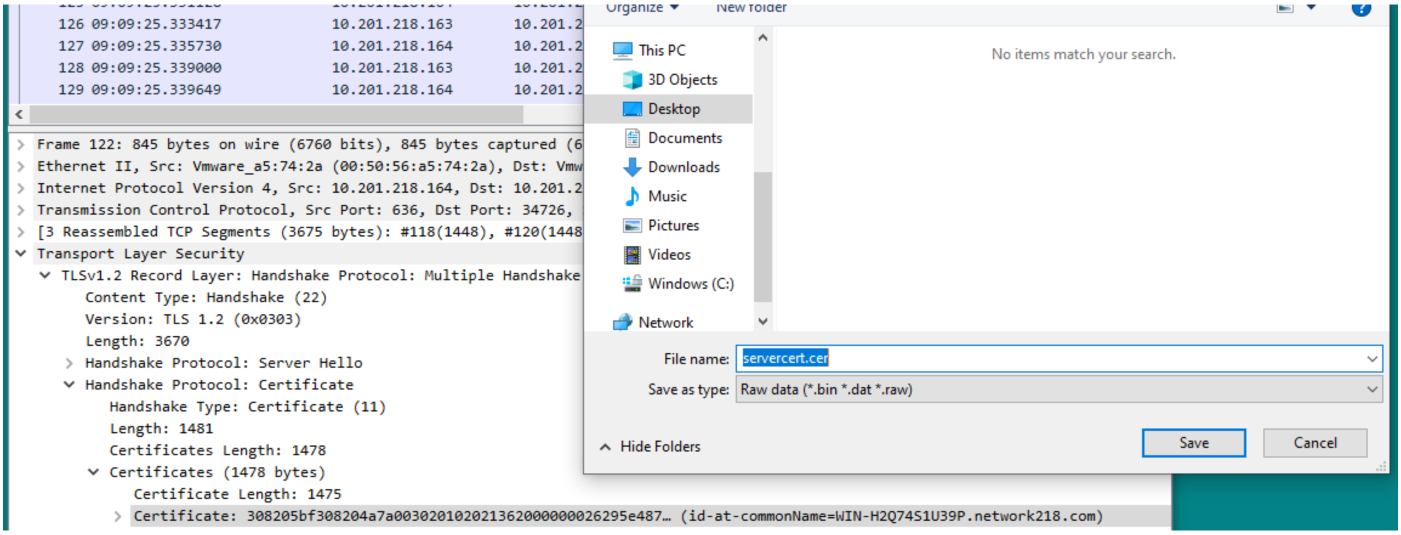


Filter: tls

```
No.   Time              Source          Destination     Protocol  Length  I
  122 09:09:25.304369   10.201.218.164  10.201.218.163  TLSv1.2   845 S
  124 09:09:25.329331   10.201.218.163  10.201.218.164  TLSv1.2   255 C
  125 09:09:25.331128   10.201.218.164  10.201.218.163  TLSv1.2   173 C
  126 09:09:25.333417   10.201.218.163  10.201.218.164  TLSv1.2   199 A
  127 09:09:25.335730   10.201.218.164  10.201.218.163  TLSv1.2   167 A
  128 09:09:25.339000   10.201.218.163  10.201.218.164  TLSv1.2   327 A
  129 09:09:25.339649   10.201.218.164  10.201.218.163  TLSv1.2   167 A
```

```
> 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
> 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: 77
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3670
    > Handshake Protocol: Server Hello
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1481
        Certificates Length: 1478
      v Certificates (1478 bytes)
          Certificate Length: 1475
        > Certificate: 308205bf308204a7a00302010202136200000026295e487… (id-at-commonName=WIN-H2Q74S1U39P.network218.com)
    > Handshake Protocol: Server Key Exchange
    > Handshake Protocol: Certificate Request
    > Handshake Protocol: Server Hello Done
```

- In the subsequent window, provide a .cer file name and then click save. The file that was saved (in this case, to the desktop) was named servercert.cer, as shown in the image:



```
  126 09:09:25.333417   10.201.218.163  10.201.2
  127 09:09:25.335730   10.201.218.164  10.201.2
  128 09:09:25.339000   10.201.218.163  10.201.2
  129 09:09:25.339649   10.201.218.164  10.201.2
```

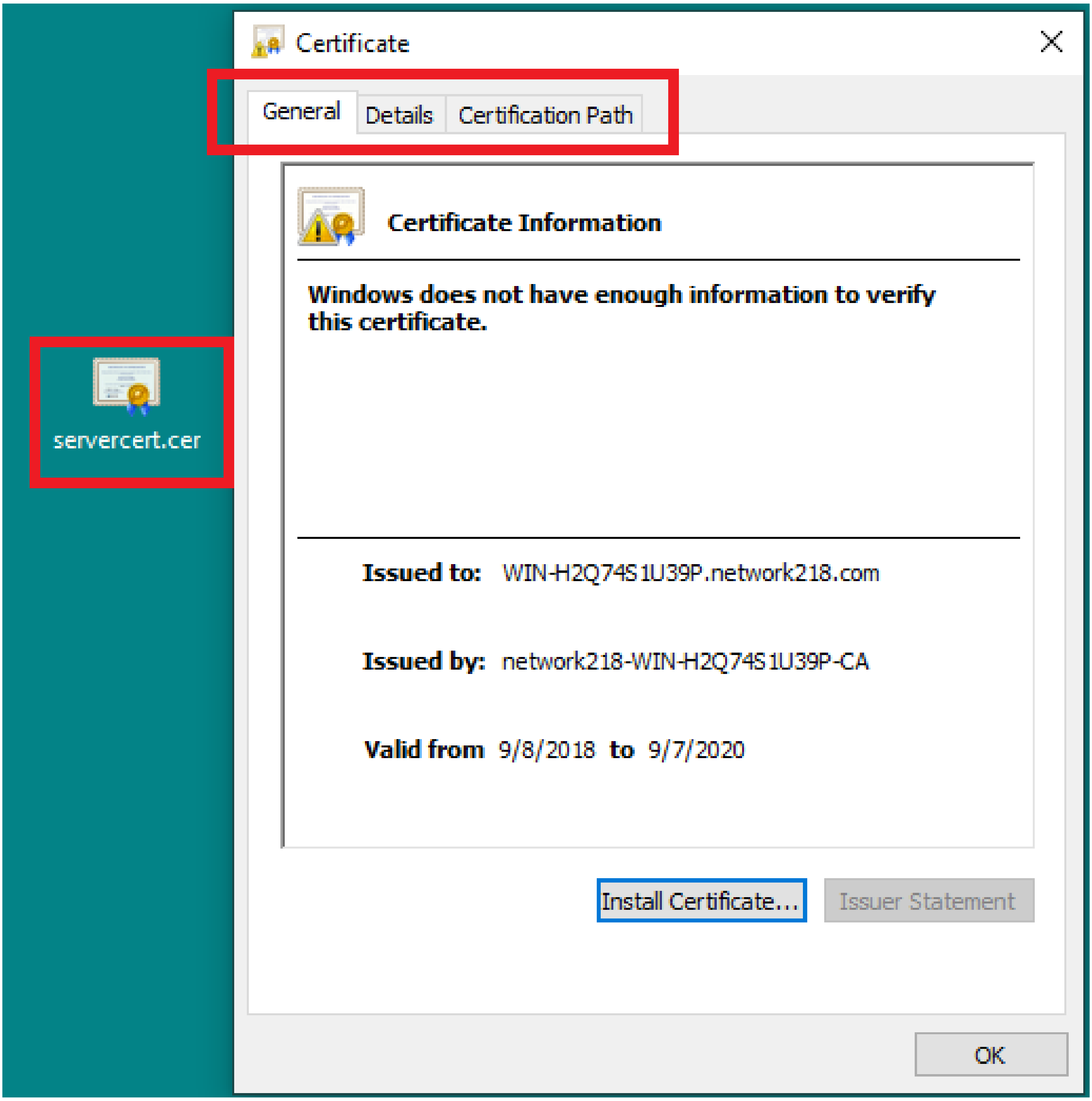
```
> Frame 122: 845 bytes on wire (6760 bits), 845 bytes captured (6
> Ethernet II, Src: Vmware_a5:74:2a (00:50:56:a5:74:2a), Dst: Vmw
> Internet Protocol Version 4, Src: 10.201.218.164, Dst: 10.201.2
> Transmission Control Protocol, Src Port: 636, Dst Port: 34726,
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3670
    > Handshake Protocol: Server Hello
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1481
        Certificates Length: 1478
      v Certificates (1478 bytes)
          Certificate Length: 1475
        > Certificate: 308205bf308204a7a00302010202136200000026295e487… (id-at-commonName=WIN-H2Q74S1U39P.network218.com)
```

File name: servercert.cer

Save as type: Raw data (*.bin *.dat *.raw)

Step 7. Open saved .CER file in order to examine contents

Double click on the .cer file in order to examine the information in the **General**, **Details** and **Certificate Path** tabs, as shown in the image:



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: WIN-H2Q74S1U39P.network218.com

Issued by: network218-WIN-H2Q74S1U39P-CA

Valid from 9/8/2018 to 9/7/2020

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.