

# ةمزمح طاققتلا نم TLS ةقداصم ري دصت ةيفيك CUCM (PCAP)

## تايوتحمل

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[CUCM PCAP نم TLS ةداهش ري دصت](#)

[ةحصللا نم ققحتلا](#)

[اهحالص او عااخال فاشكتسا](#)

## ةمدقملا

CISCO Unified Communications Manager (CUCM) نم ةداهش ري دصت ءارج دننتمسمل اذه فصوي PCAP.

Cisco نم TAC سدنهم، وللي كسإ ناي ردا ةطساوب ةمهاسملا تمت

## ةيساسأل تابلطتملا

### تابلطتملا

ةيلالتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

· (TLS) لقنلا ةقبط ناما ةحفاصم:

· CUCM تاداهش ةرادا:

· (SFTP) نمأل تافللملا لقن لوكونورب مداخ:

· (RTMT) يلعفلا تقولا ةبقارم ةادا:

· Wireshark قيبطت

### ةمدختسملا تانوكملا

· ثدخال تارادصل او 9.x رادصلال CUCM

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دننتمسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتمسمل اذه يف ةمدختسملا ةزهجال عيمج تادب رمايال لمتمحمل ري ثاتلل كمهف نم دكأتف، ليغش تال دي قكتكبش

## ةيساسأ تامولعم

تاداهش/تاداهش ةلسلس ةقباطم ديكتل مداخال تاداهش/تاداهش ةلسلس ري دصت نكمي  
إلا اهلي محت مت يتلا وأ اهلي محت مت يتلا (تاداهشلا) ةداهشلل مداخال اهرفوي يتلا مداخال

CUCM تاداهش ةرادإ

CUCM إلی مداخل ةداهش/ةداهش ةلسلس مداخل رفوی، TLS دیکأت نم ءزجک

## CUCM PCAP نم TLS ةداهش ریدصت

CUCM یلع ةمزحلا طاقنلا رمأ ءدب 1. ةوطخل

فلم مادختساب رمأ لایغش تب مقو CUCM ةدقعب (SSH) ةنمآ ةرشق لاصتا ءاشناب مق ةروصلایف حضورم وه امك، all مجح 1000000 ددع (rotate-طاقنلا و) ةكبشلا طاقنلا <filename>

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

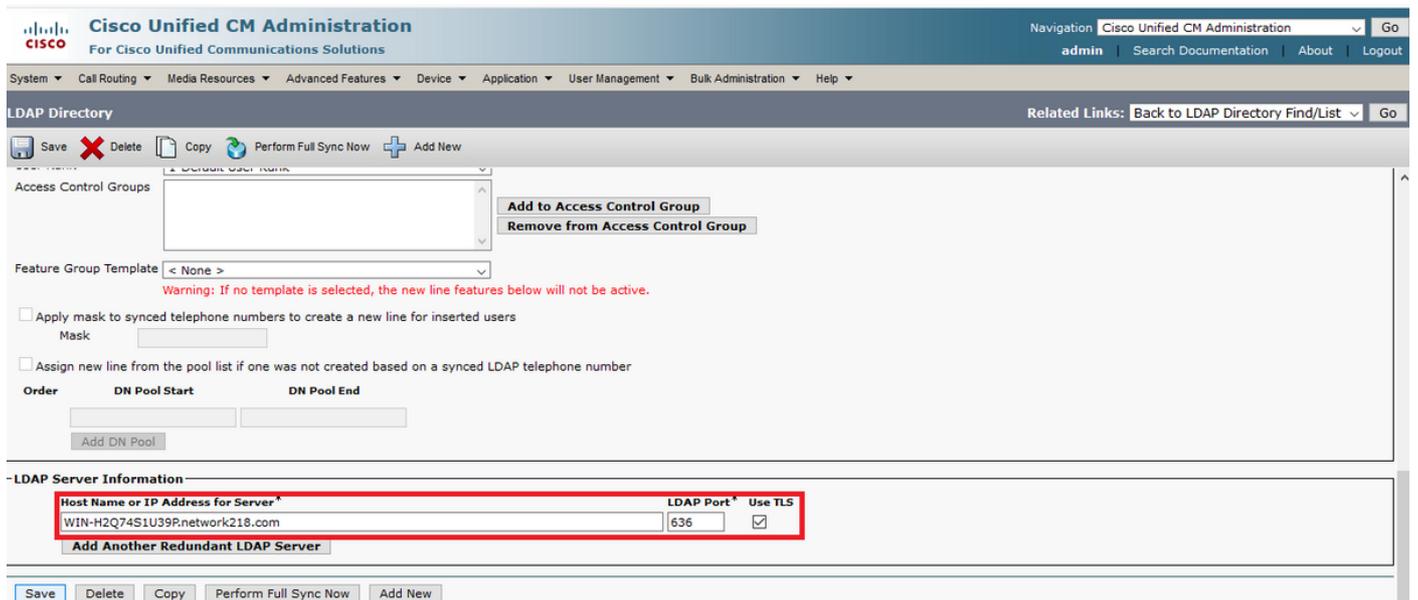
Welcome to the Platform Command Line Interface

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=
```

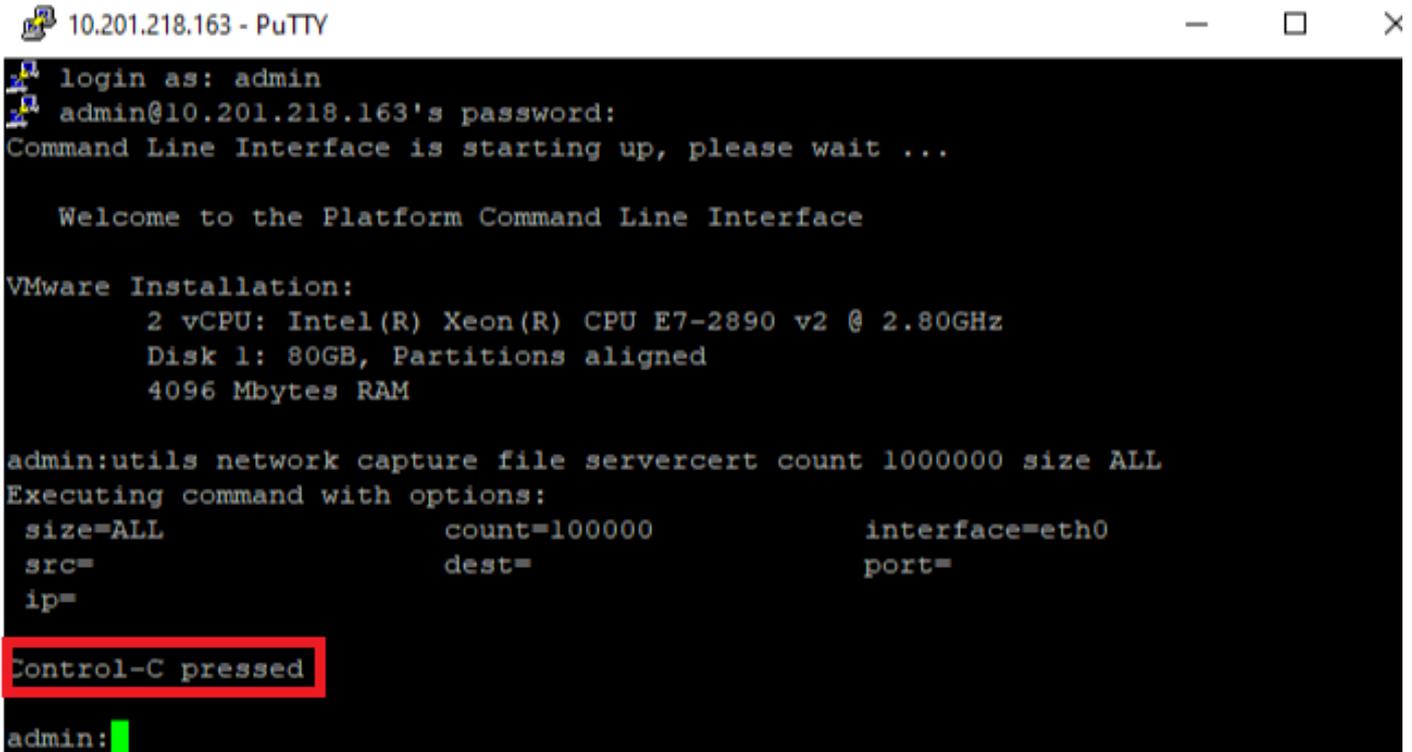
CUCM و مداخل نیب TLS لاصتا ءدب 2. ةوطخل

(LDAP) لیلدلا یلا نمآلا لوصولا لوكوتورب مداخل نیب TLS لاصتا أدبت، لاثملا اذه یف ةروصلایف حضورم وه امك، TLS 636 ذفنم یلع لاصتا ءاشناب لالخ نم (CUCM) Lightweight



TLS ءحفاصم لامك اءب CUCM PCAP فاقي ا. 3 ءوطالا

ءروصلا يف ءضوم وه امك ، ءمزالا طاقالا فاقي اءب Control-C لىل طغضا



```
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=

Control-C pressed

admin:█
```

نيت ءورسمل انيتقي رطلال نم يا ما ءءسا با ءئب ءالا ءا ءا طاقالا فلم ليزنبا مق 4. ءوطالا

لءس & ءببا > ءببا > اءا > ماظن لىل لقاانا و CUCM ءءقل RTMT لىل ءببا مق 1. ليزنبا ل RTMT ءل لءم ءالا نم ءباا) مزالا طاقالا اءس ءببم ءءو اءلما ءمء > يزكرم PCAP) ءروصلا يف ءضوم وه امك :

Collect Files

Select System Services/Applications

Select all Services on all Servers

Name	All Servers	<input type="checkbox"/> cucmpub216.network...	<input type="checkbox"/> imp216.network2
PIPS Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Host Resources Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CLI Created Reports	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CLI Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform Cert Monitor Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform CertMgr Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform Cluster Manager Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform GUI Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform IPSecMgmt Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IPT Platform RemoteSupport Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install File Signing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Install and Upgrade Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerneldump Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MIB2 Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mail Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mgetty Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTP Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packet Capture Logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Prog Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAR Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SELinux logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Master Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Service Registration Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spooler Logs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Application Agent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

< Back   Next >   Finish   Cancel

2. مق، CUCM SSH ةسلج يفو (SFTP) نمآلا تافللملا لقن لوكوتورب مداخ ليغشت أدبا. رماوآلا تاهجوم لالخنم رمتسا) `get activelog /patform/cli/<pcap filename>.cap` رمالا ليغشتب ةروصلا يف حضوم وه امك، (SFTP) مداخ يلع PCAP ليزنل

```

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=

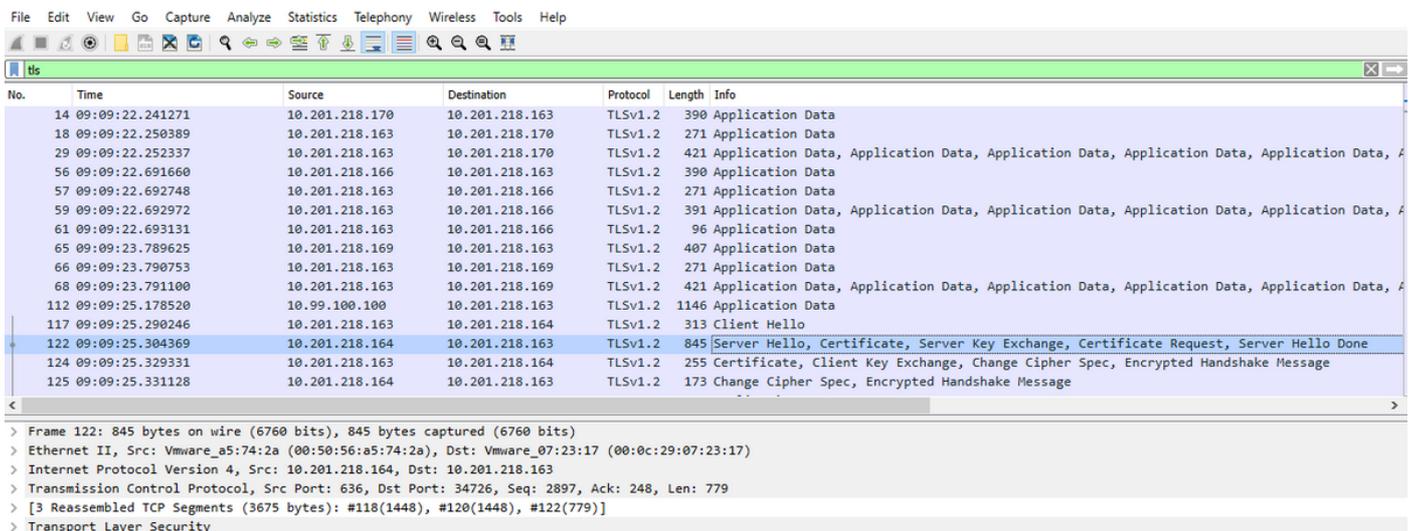
Control-C pressed

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]?

```

مداخل لبق نم CUCM إلى مدمقم ال تاداهش ال دد دي دحت 5. ووطخل

يت ال مزل ال دي دحت ال TLS إلى عي فصت ال لماع و PCAP حت فل Wireshark قي ببطت م دخت س أ CUCM. إلى مدمقم ال مداخل ال داهش / داهش ال سلس إلى عي وحت يت ال Server Hello إلى عي وحت ال :ةروصل ال في حضورم وه امك ، 122 راطا اذه



ةداهش ال عم مداخل ال ابحرم ةمزل نم ةداهش ال تامولعم > لقنل ال ةقبط ني مات عي سوتب مق ةلاجل ال هذه في .مداخل ال داهش يه ال لعل ال داهش ال CUCM. إلى مدمقم ال تاداهش ال دد دي دحت ال :ةروصل ال في حضورم وه امك طقف ةدحاو مداخل ال داهش ضرع متي

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

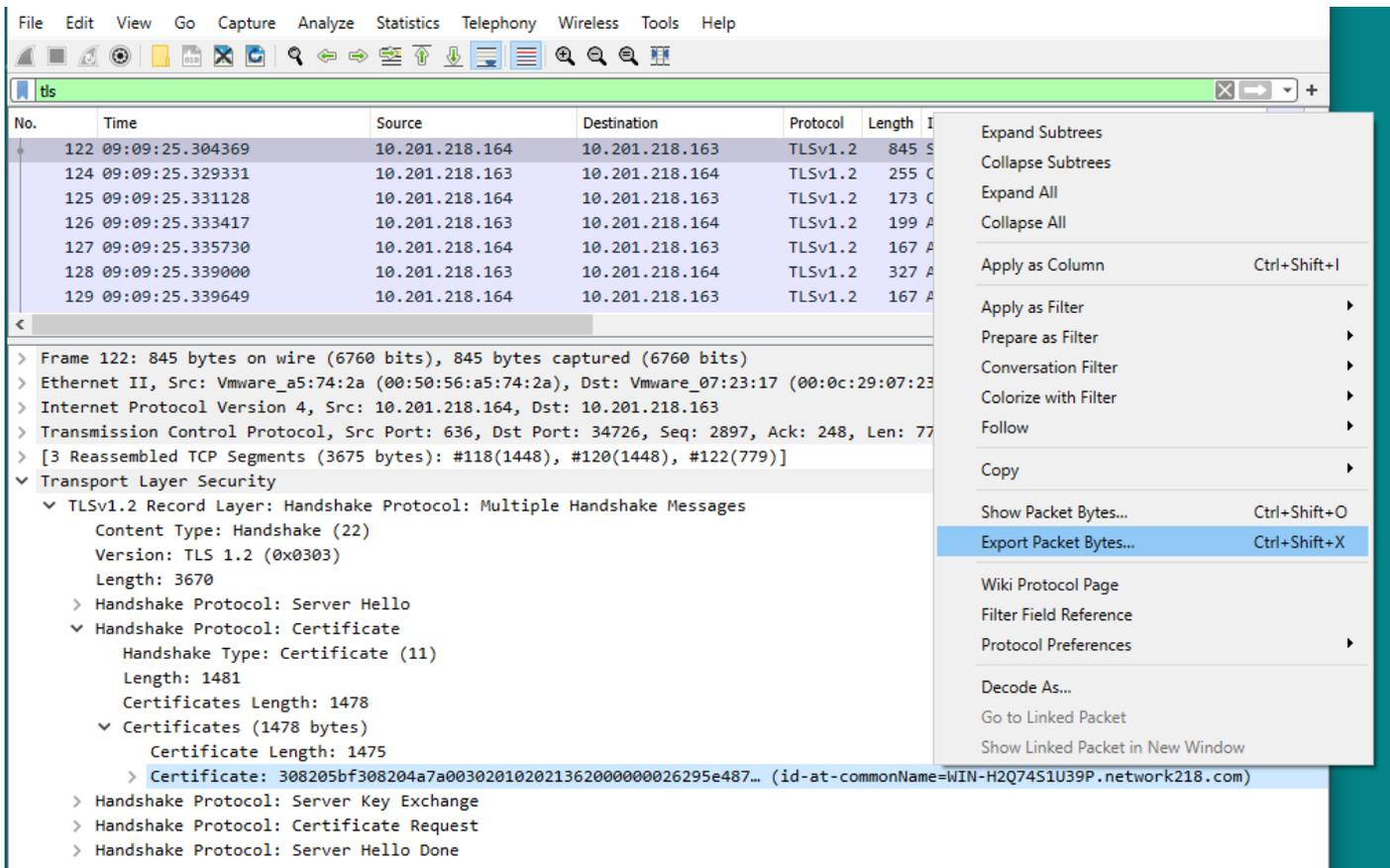
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]

Transport Layer Security

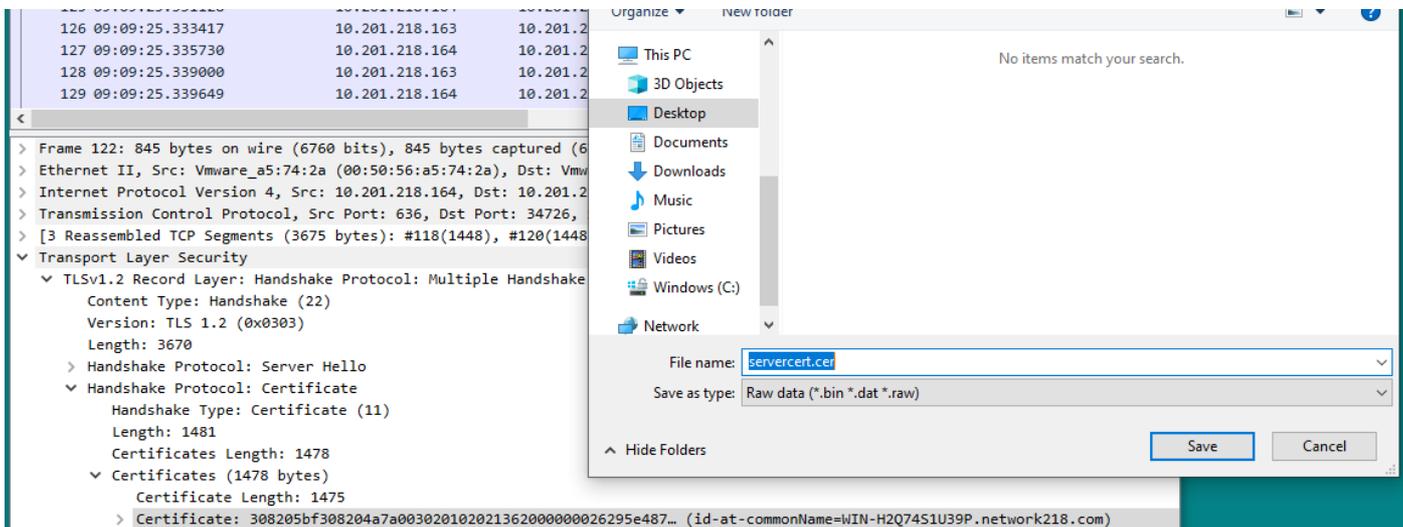
- TLsv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 3670
  - Handshake Protocol: Server Hello
  - Handshake Protocol: Certificate
    - Handshake Type: Certificate (11)
    - Length: 1481
    - Certificates 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

CUCM PCAP نم مداخل تاداهش/تاداهش ةلسلس ري دصت 6. ةوطخل

ررب رقنا .مداخل ةداهش صرحت لى لجاتحت ك لذل ، طقف مداخل ةداهش ضرع متي ، لاثملا اذه يف وه امك ، .cer ةداهشك ظفحل مزحلا تياب تادجور يدصت دحو مداخل ةداهش لى نميال سواملا ةروصلال يف حضورم :

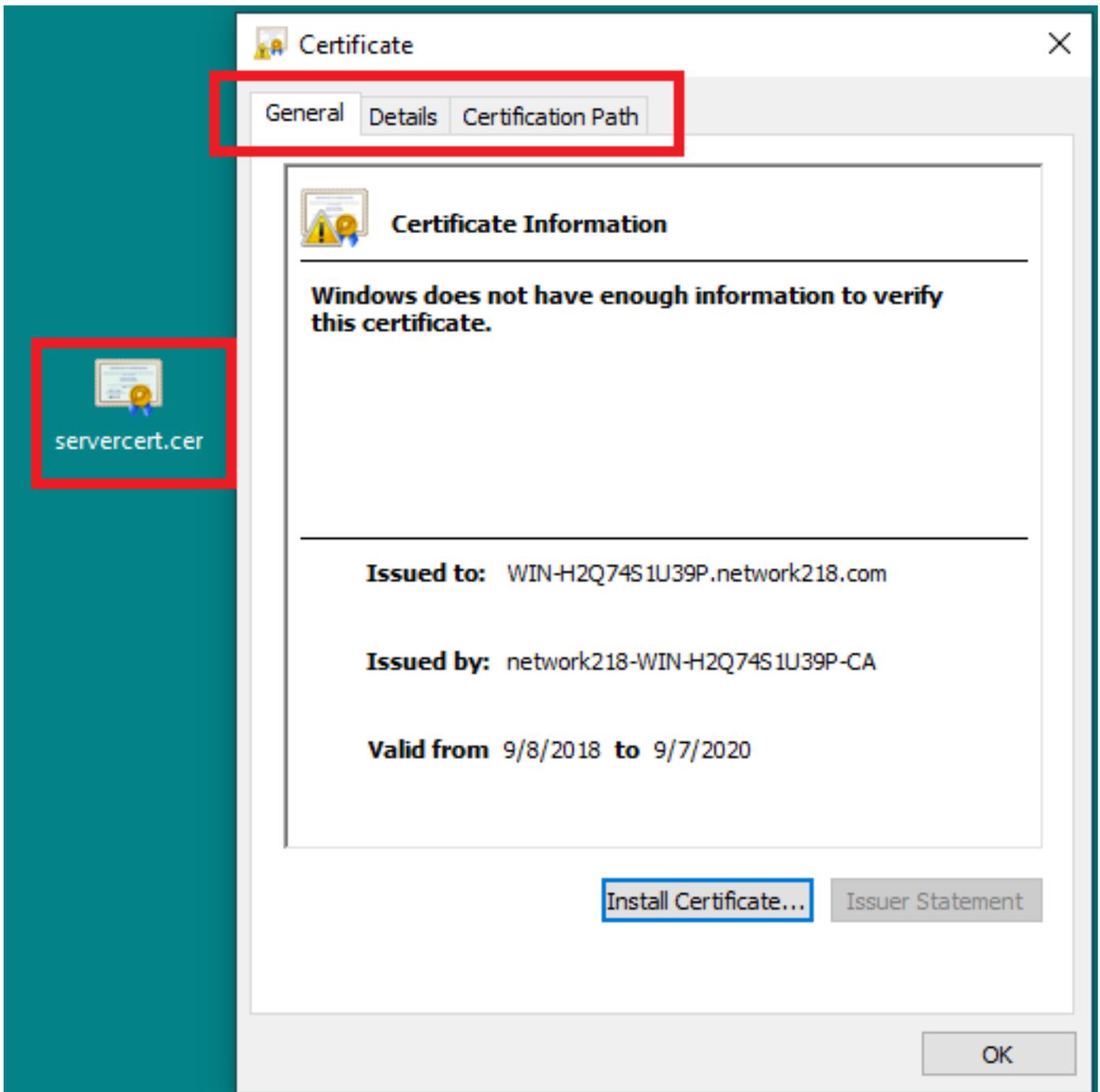


يذال فلم الةيمست مت .ظفح قوف رقنا مث cer. فلم مساري فو تب مق ،ليل ال راطال ايف .ةروصل ايف حضورم وه امك ،servercert.cer مساب (بكت الما حطس لى ،ةالاحل هذه يف) هظفح مت



تايوت حمل الصحف لجا نم ظوف حمل ال CER. فلم حتف 7. ةوطخل

للي صافات ل اوامع بي وبت ال تامال ع يف تامول عمل الصحف cer. فلم لى ع اچودزم ارقن رقنا .ةروصل ايف حضورم وه امك ،ةداهش ال راسمو



## ةحصللا نم ققحتلا

نڤوكتلا اذه ةحص نم ققحتلل ءارجا ايلاح دجوي ال

## اهحالصاو ءاطخال فاشكتسا

نڤوكتلا اذهل اھحالصاو ءاطخال فاشكتسال ةددم تامولعم ايلاح رفوتت ال

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد ىوتحم مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتحم مچرت مء مء دقء ةل  
ىل ةمءءاد ةوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل ةل ةل ةل  
(رفوتم طبارل) ةل صأل ةل ةل