

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

## تايتوتحملا

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[CUCM PCAP نم TLS ةداهش ري دصت](#)

[ةحصللا نم ققحتلا](#)

[اهالصل او ءاطخال افاشكتسا](#)

## ةمدقملا

CISCO Unified Communications Manager (CUCM) نم ةداهش ري دصت ءارج دننتملا 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 نام ةحفاصم:

· CUCM تاداهش ةرادا:

· (SFTP) نمأل تافللملا لقن لوكونورب مداخ:

· (RTMT) يلعفل تاقولا ةبقارم ةادا:

· Wireshark قيبطت:

### ةمدختسملا تانوكملا

· ثدخال تارادصل او 9.x رادصلال CUCM

ةصاخ ةيلعم ةئيب يف ةدوجوملا ةزهجال نم دننتملا اذه يف ةدراول تامولعملا ءاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتملا اذه يف ةمدختسملا ةزهجال عيمج تادب رمأ يال لمتمحملا ري ثاتلل كمهف نم دكأتف، ليغشنتلا ديقت كتكبش

## ةيساسأ تامولعم

تاداهش/تاداهش ةلسلس ةقباطم ديكتل مداخل تاداهش/تاداهش ةلسلس ري دصت نكمي  
إلا اهليمحت مت يتلا وأ اهليمحت مت يتلا (تاداهشلا) ةداهشلل مداخل اهرفوي يتلا مداخل

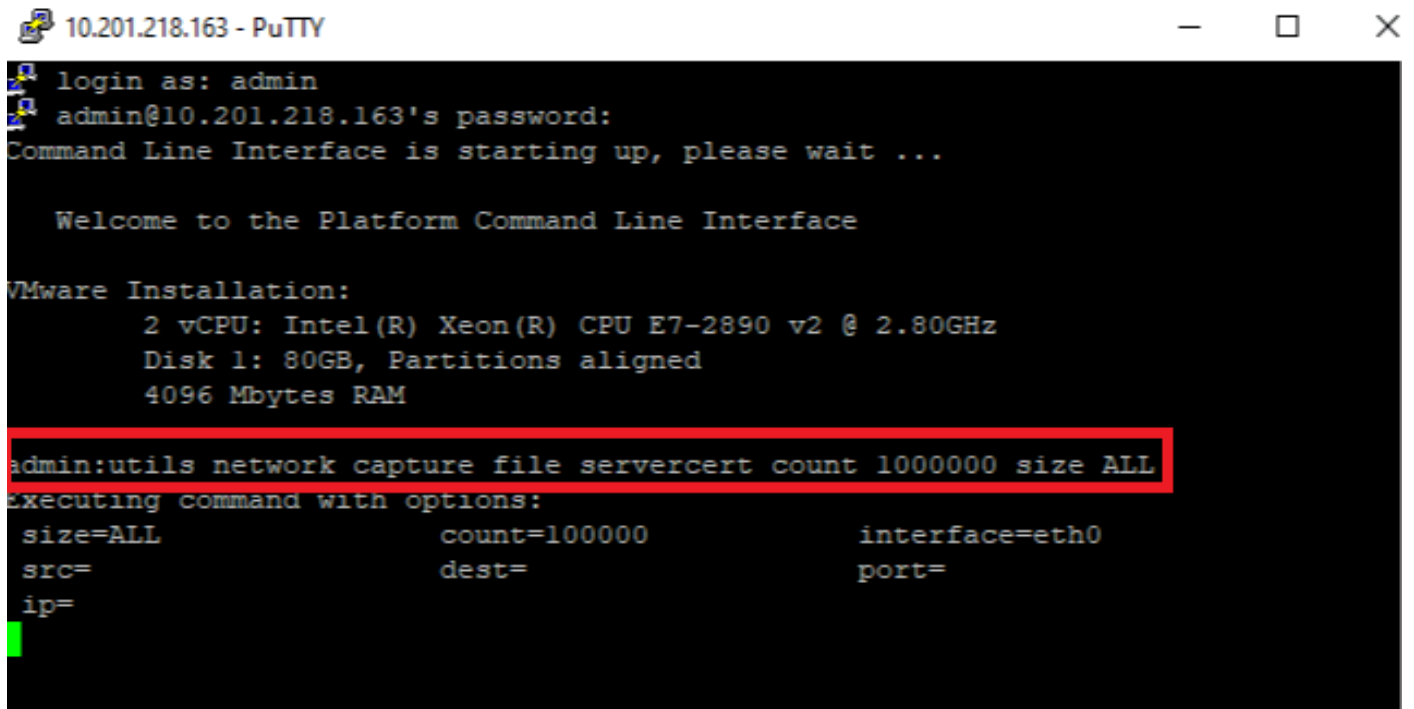
CUCM تاداهش ةرادإ

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

## CUCM PCAP نم TLS ةداهش ریدصت

CUCM یلع ءمزحلا طاقنلا رمأ ءدب 1. ءوطخل

فلم مادختساب رمألا لیغشتب مقو CUCM ءدقعب (SSH) ءنمآ ءرشق لاصتا ءاشناب مق ءروصلایف ءضوم وه امك، all مءج 1000000 ددع (rotate-طاقنلا و) ءكبشلا 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 ...

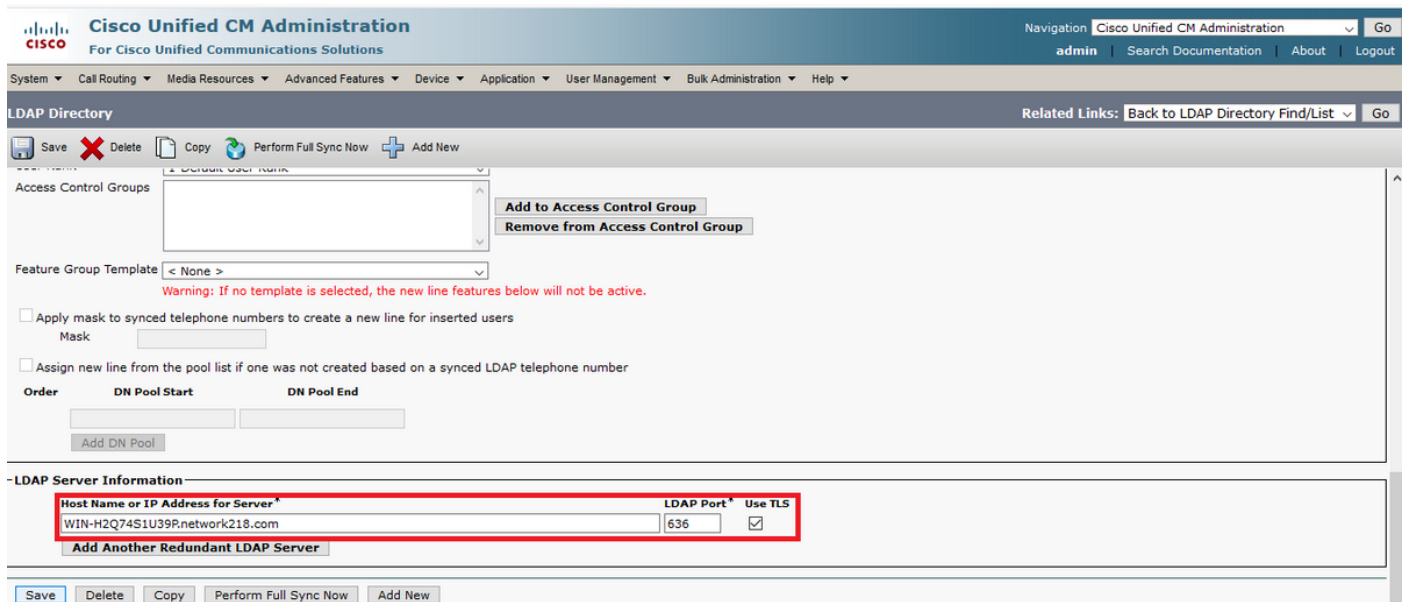
Welcome to the Platform Command Line Interface

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=
```

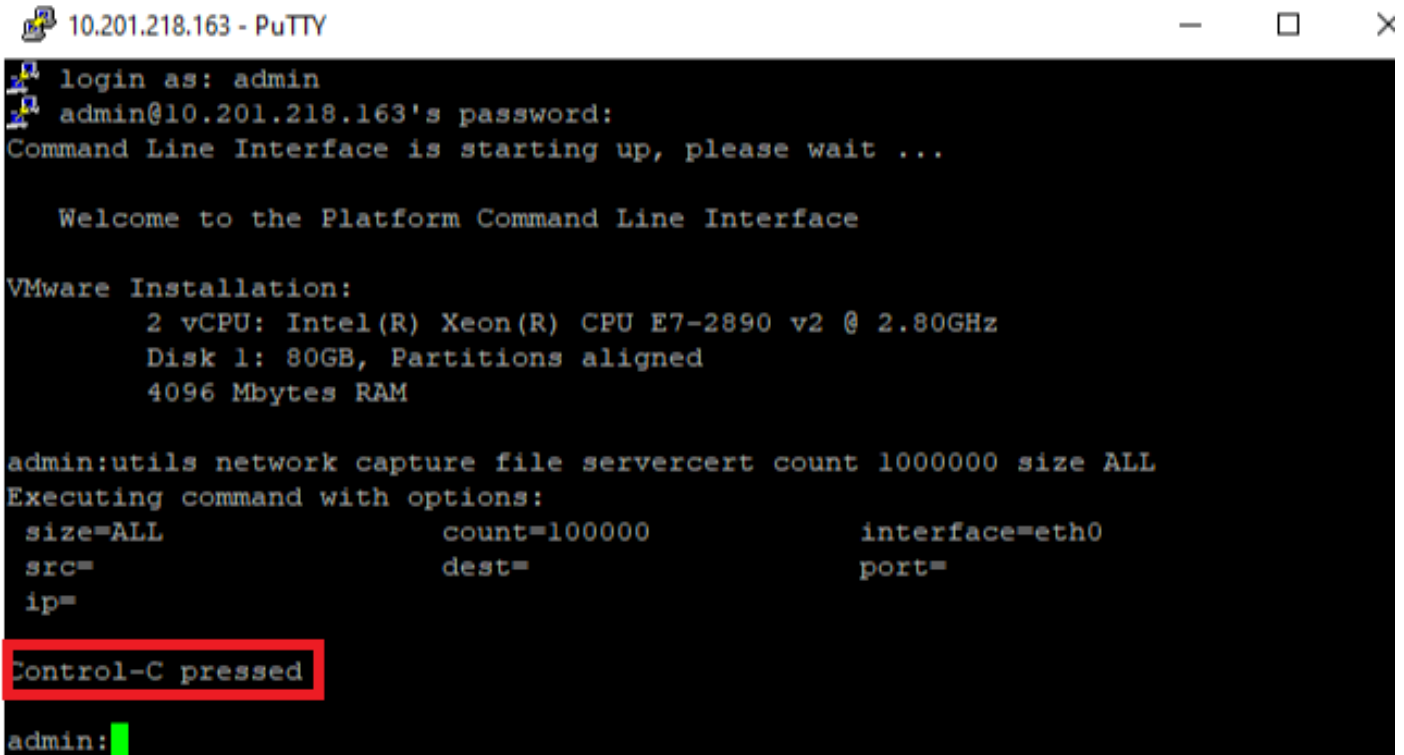
CUCM و مداخل نیب TLS لاصتا ءدب 2. ءوطخل

(LDAP) لیلدلا یلا نمآلا لوصولا لوكوتورب مءاخ نیب TLS لاصتا أدبت، لاثملا اءه یف ءروصلایف ءضوم وه امك، TLS 636 ذفنم یلع لاصتا ءاشناب لالء نم (CUCM) Lightweight



TLS ةحفاصم لامك| دعب CUCM PCAP فاقې| 3. ةوطخلا

ةروصلال ي ف حضورم وه امك ،ةمزحلا طاقتلا فاقې| Control-C لىل ع 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 دورسملال ني تقي رطلال نم ي ا مادختساب ةئبعتلا ةادأ طاقتلا فلم ليزنتب مق 4. ةوطخلا

لجس & عبتت > عبتت > تاودأ > ماظن لىل لقتناو CUCM ةدقعل RTMT لىل غشبتب مق 1. ليزنتل RTMT ةللمع لال خ نم عبات) مزحلا طاقتلا تالجس ع برم ددحو تافلما عمج > يزكرم PCAP، ةروصلال ي ف حضورم 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 ىلع 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

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

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

ءداهش ال عم مداخل ابحرم ةمزل نم ةداهش ال تامول عم > لقنل ال ةقبط ني مات عي سوتب مق ةلاجل هذه في .مداخل ةداهش يه ايل ال ةداهش ال CUCM. إلى مدمقم ال تاداهش ال دد دي دحت ةروصل ال في حضورم وه امك طقف ةدحاو مداخل ةداهش 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

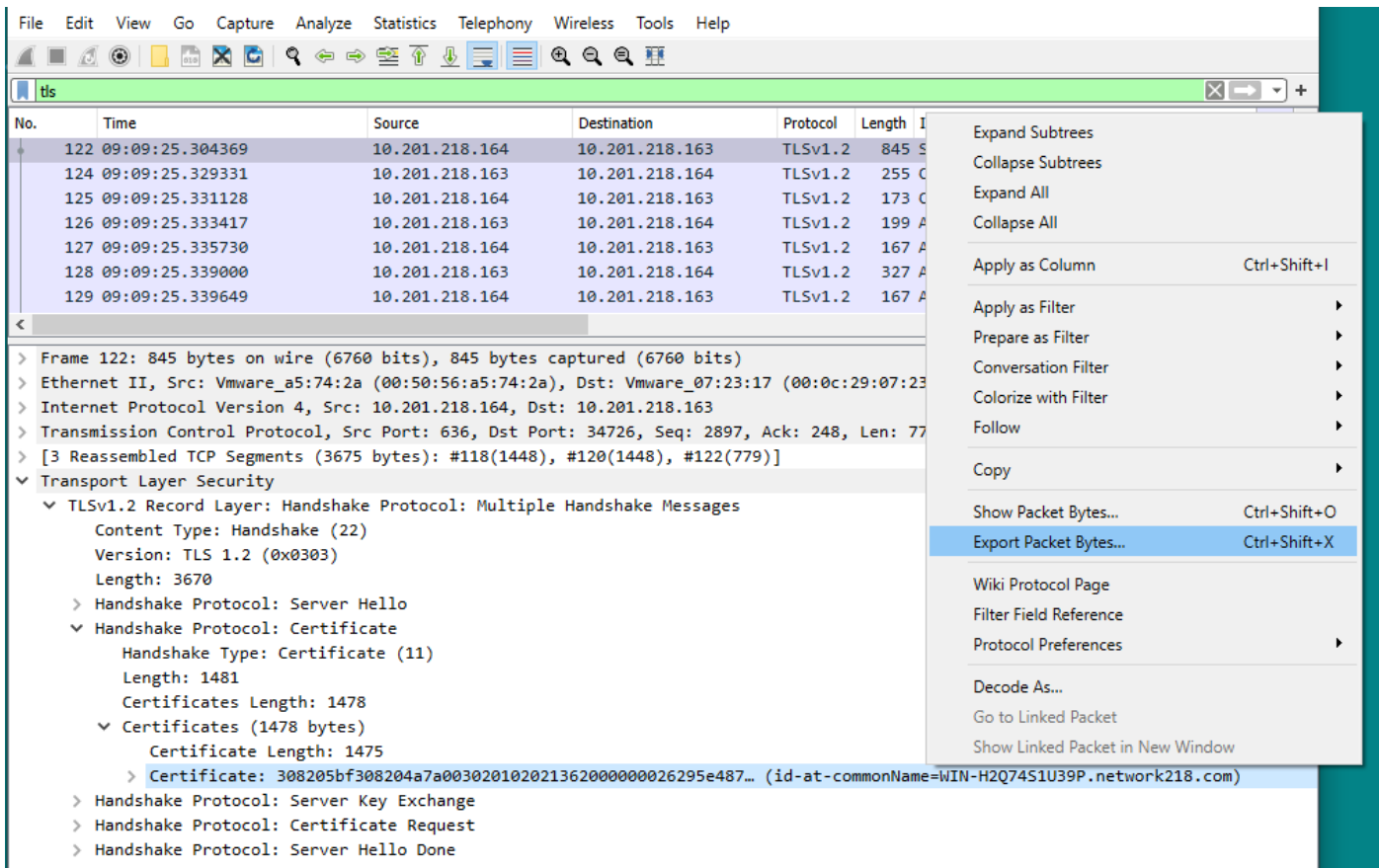
> [3 Reassembled TCP Segments (3675 bytes): #118(1448), #120(1448), #122(779)]

Transport Layer Security

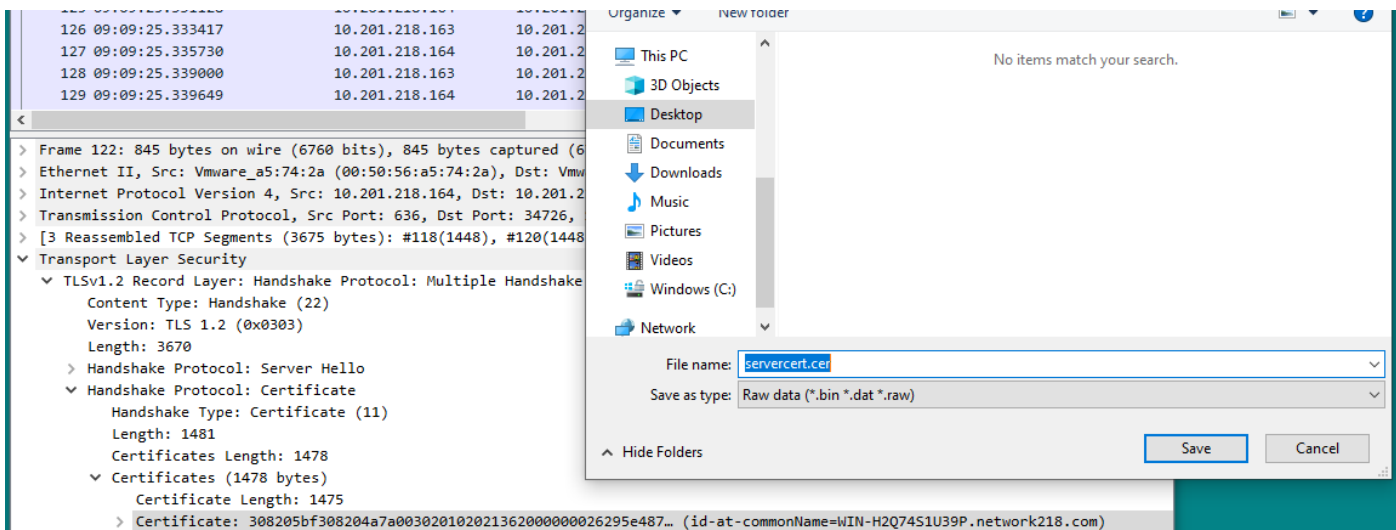
- TLsv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 3670
  - Handshake Protocol: Server Hello
  - Handshake Protocol: Certificate
    - Handshake Type: Certificate (11)
    - Length: 1481
    - Certificates 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 صحف لى لجاتحت كلذل ، طقف مداخل ةداهش ضرع متي ، لاثملا اذه يف وه امك ، .cer. ةداهشك ظفحلل مزحلل تاياب تادج وري دصت دحو مداخل ةداهش لىل نميال سواملا ةروصلال يف حضورم:

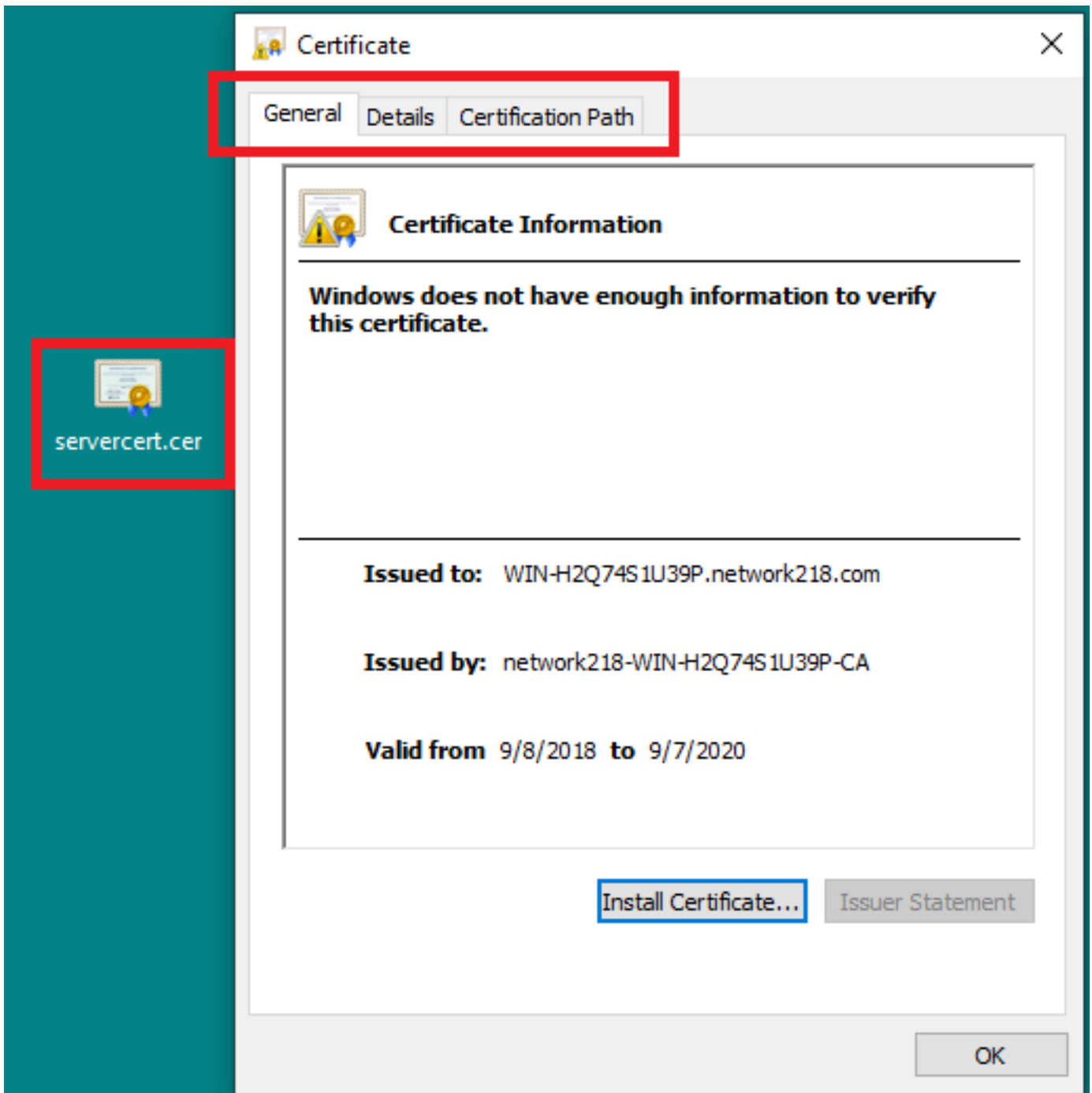


يذال فلم الةيمست مت .ظفح قوف رقنا مث cer. فلم مساري فو تب مق ،ليل ال راطال ايف .ةروصل ايف حضورم وه امك ،servercert.cer مساب (بكت الما حطس لى ،ةالاحل هذه يف) هظفح مت



تايوت حمل ال صحف لجأ نم ظوف حمل ال CER. فلم حتف 7. ةوطخل

لئصافت ال اوامع بي وبت ال تامال ع يف تامول عمل ال صحف فل 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 اءحالصاو 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 و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل