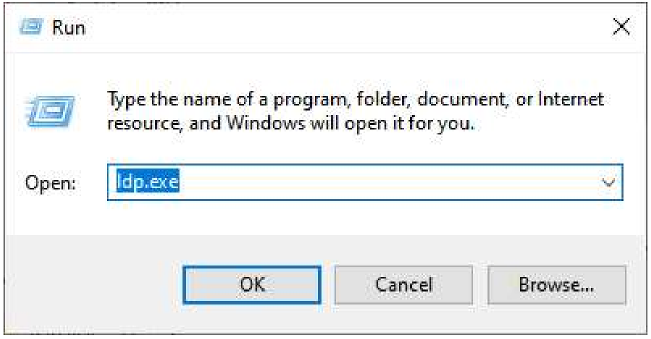
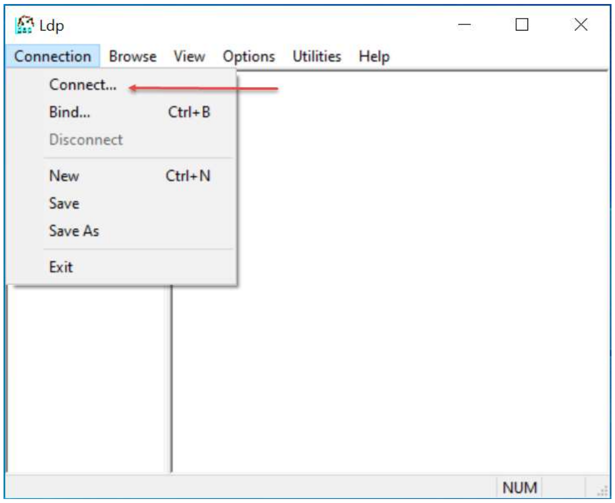
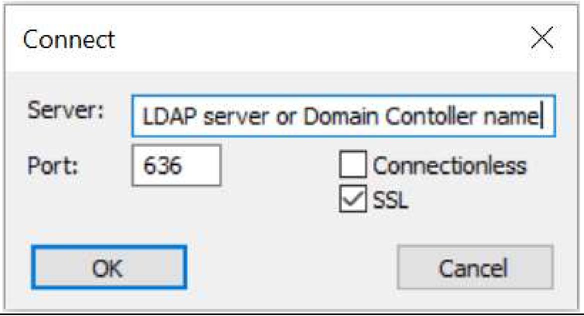
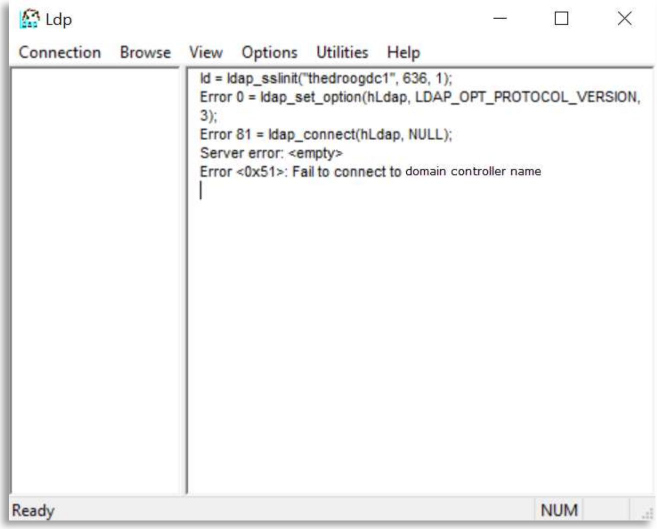
Determine if LDAP server is permitting binds via LDAPS using LDP.exe

Test Domain: TheDroog.droog
Client: Windows 10 with RSAT tools installed (IP address: 192.168.72.10)
LDAP/Domain Controller: Windows Server 2016 Domain Controller (IP address: 192.168.72.100)

Run ldp.exe	1.) Click start > Run 2.) Open ldp.exe (included with Windows 10 Remote Server Admin tools)  Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: ldp.exe
	3.) Click Connection > Connect  Ldp Connection Browse View Options Utilities Help Connect... Bind... Ctrl+B Disconnect New Ctrl+N Save Save As Exit NUM
	4.) Server = Your LDAP server name or DC Port = 636 SSL checkbox checked  Connect Server: LDAP server or Domain Contoller name Port: 636 ☐ Connectionless ☑ SSL

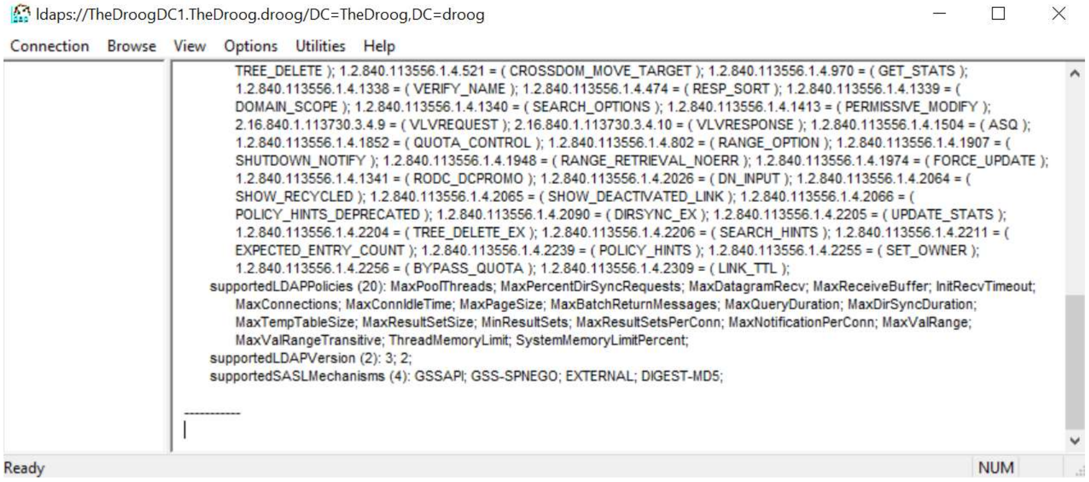
5.) Unsuccessful connection:



```
ld = ldap_sslinit("thedroogdc1", 636, 1);
Error 0 = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION,
3);
Error 81 = ldap_connect(hLdap, NULL);
Server error: <empty>
Error <0x51>: Fail to connect to domain controller name
```

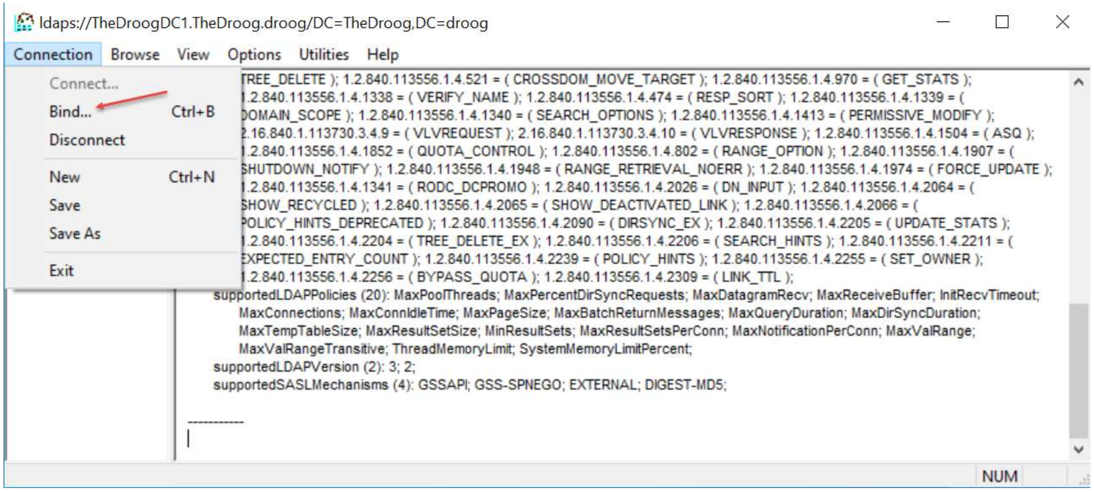
This indicates that there is no valid certificate facilitating LDAPS requests. Steps would need to be taken to install/configure a certificate (outside of the scope of this document), but a good tutorial for reference:
https://www.youtube.com/watch?v=JFPa_uY8NhY

6.) Successful connection via LDAPS:

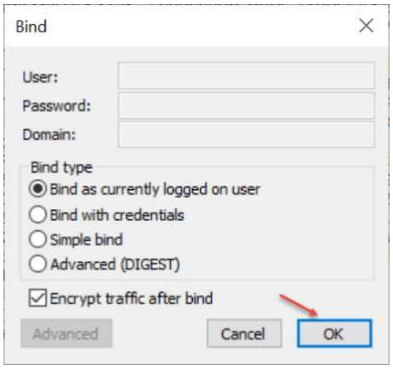

ldaps://TheDroogDC1.TheDroog.droog/DC=TheDroog,DC=droog
Connection Browse View Options Utilities Help
Ready
NUM

```
        TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS );
        1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = (
        DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY );
        2.16.840.1.113730.3.4.9 = ( VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ );
        1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = (
        SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE );
        1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = (
        SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = (
        POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX ); 1.2.840.113556.1.4.2205 = ( UPDATE_STATS );
        1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = (
        EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS ); 1.2.840.113556.1.4.2255 = ( SET_OWNER );
        1.2.840.113556.1.4.2256 = ( BYPASS_QUOTA ); 1.2.840.113556.1.4.2309 = ( LINK_TTL );
    supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout;
        MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration;
        MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
        MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

7.) Test an LDAPS Bind:


ldaps://TheDroogDC1.TheDroog.droog/DC=TheDroog,DC=droog
Connection Browse View Options Utilities Help
Connect...
Bind... Ctrl+B
Disconnect
New Ctrl+N
Save
Save As
Exit
NUM

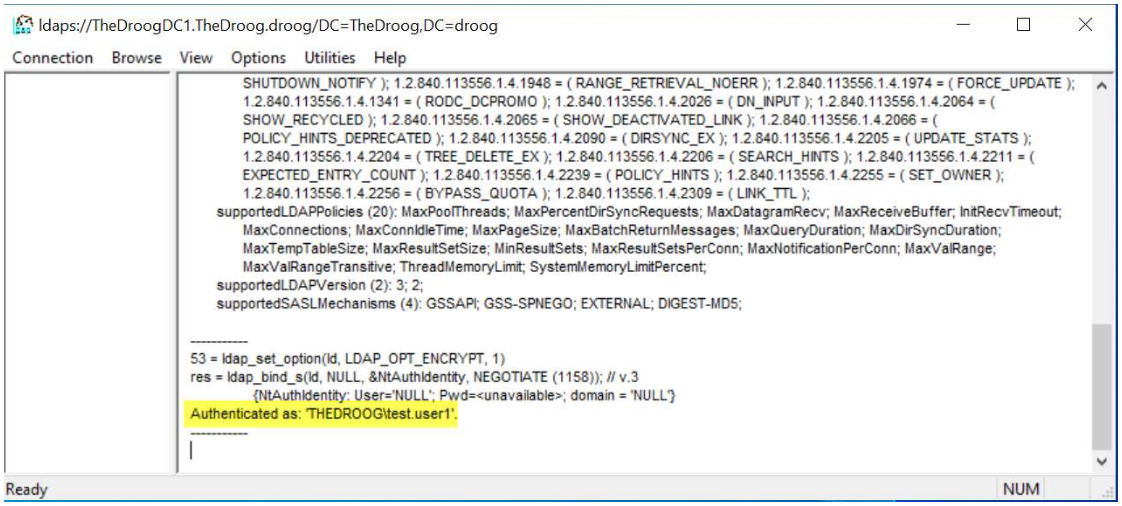
```
 TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS );
 1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = (
 DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY );
 2.16.840.1.113730.3.4.9 = ( VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ );
 1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = (
 SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE );
 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = (
 SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = (
 POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX ); 1.2.840.113556.1.4.2205 = ( UPDATE_STATS );
 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = (
 EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS ); 1.2.840.113556.1.4.2255 = ( SET_OWNER );
 1.2.840.113556.1.4.2256 = ( BYPASS_QUOTA ); 1.2.840.113556.1.4.2309 = ( LINK_TTL );
supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout;
    MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration;
    MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
    MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```



User:
Password:
Domain:

Bind type
● Bind as currently logged on user
○ Bind with credentials
○ Simple bind
○ Advanced (DIGEST)

☑ Encrypt traffic after bind

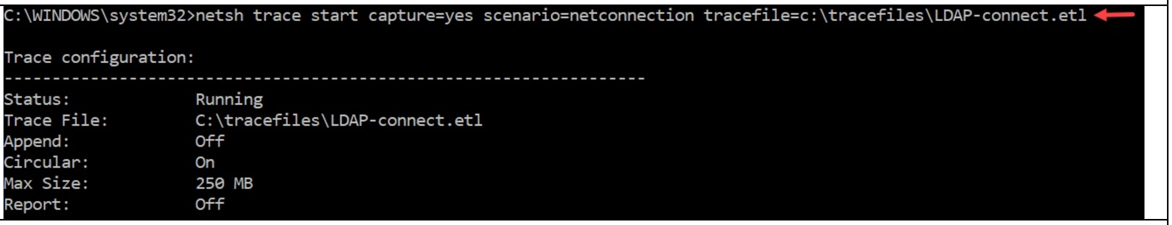

ldaps://TheDroogDC1.TheDroog.droog/DC=TheDroog,DC=droog
Connection Browse View Options Utilities Help
Ready
NUM

```
        SHUTDOWN_NOTIFY ); 1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE );
        1.2.840.113556.1.4.1341 = ( RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = (
        SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = (
        POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX ); 1.2.840.113556.1.4.2205 = ( UPDATE_STATS );
        1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = (
        EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS ); 1.2.840.113556.1.4.2255 = ( SET_OWNER );
        1.2.840.113556.1.4.2256 = ( BYPASS_QUOTA ); 1.2.840.113556.1.4.2309 = ( LINK_TTL );
    supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout;
        MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration;
        MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange;
        MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
53 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); // v.3
        {NtAuthIdentity: User='NULL'; Pwd=<unavailable>; domain = 'NULL'}
Authenticated as: 'THEDROOG\test.user1'.
-----------
```

Bind via LDAPS is successful

Using Microsoft Network Monitor 3.4 to determine which Cert is performing LDAPS binds

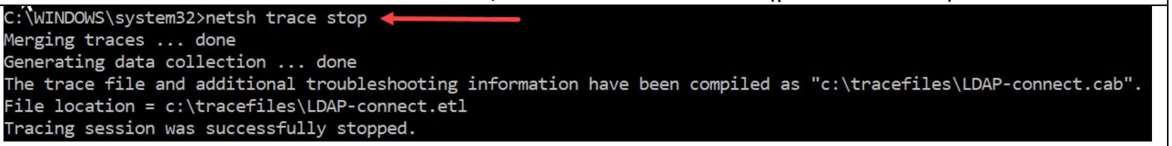
On client computer Start a trace



```
C:\WINDOWS\system32>netsh trace start capture=yes scenario=netconnection tracefile=c:\tracefiles\LDAP-connect.etl

Trace configuration:
-------------------------------------------------------------------
Status:             Running
Trace File:         C:\tracefiles\LDAP-connect.etl
Append:             Off
Circular:           On
Max Size:           250 MB
Report:             Off
```

On client computer establish an LDAPS connection to the LDAP/DC server via LDP.exe (process above)

After successful LDAPS connection via LDP.exe stop trace



```
C:\WINDOWS\system32>netsh trace stop
Merging traces ... done
Generating data collection ... done
The trace file and additional troubleshooting information have been compiled as "c:\tracefiles\LDAP-connect.cab".
File location = c:\tracefiles\LDAP-connect.etl
Tracing session was successfully stopped.
```

Open tracefile in Microsoft Network Monitor 3.4

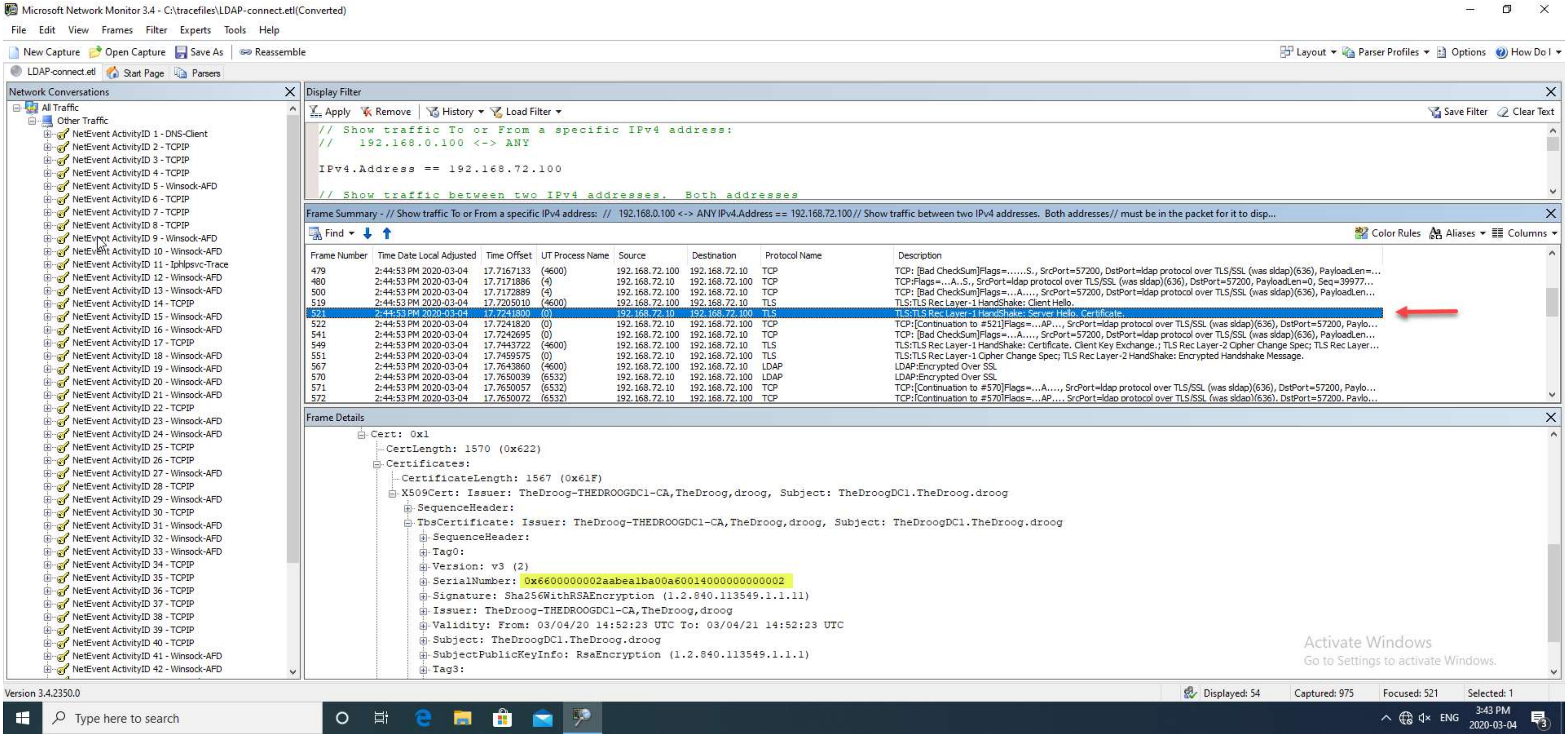
1.) File > Open > Capture: browse to trace-file.
2.) After tracefile is loaded, if error “Requires full common parsers…” is encountered
    i) Tools > Options
    ii) Parser Profiles Tab
    iii) In available Parser Profiles window > Right click Windows > Set as Active.
3.) Load IPv4 standard filter and filter for the IP of the LDAP/DC server
4.) Scroll through the Frames to find the handshake between client IP and DC IP with description:

TLS:TLS Rec Layer-1 HandShake: Server Hello. Certificate

5.) In the bottom Frame Details pane, navigate through the nested details to:

TLS > TlsREcordLayer: TLS Rec Layer-1 Handshake: > SSLHandshake: SSL HandShake Certificate (0x0B) > Cert: 0x1 > Certificates: > X509: Issuer…*DC info* > TbsCertificate: Issuer: *DC info* > Make note of Serial Number (We will compare it to the SN# in the MS Personal Certificate store)

Serial Number in this example = 0x6600000002aabealba00a60014000000000002



```
All Traffic
  Other Traffic
    NetEvent ActivityID 1 - DNS-Client
    NetEvent ActivityID 2 - TCPIP
    NetEvent ActivityID 3 - TCPIP
    NetEvent ActivityID 4 - TCPIP
    NetEvent ActivityID 5 - Winsock-AFD
    NetEvent ActivityID 6 - TCPIP
    NetEvent ActivityID 7 - TCPIP
    NetEvent ActivityID 8 - TCPIP
    NetEvent ActivityID 9 - Winsock-AFD
    NetEvent ActivityID 10 - Winsock-AFD
    NetEvent ActivityID 11 - Iphlpsvc-Trace
    NetEvent ActivityID 12 - Winsock-AFD
    NetEvent ActivityID 13 - Winsock-AFD
    NetEvent ActivityID 14 - TCPIP
    NetEvent ActivityID 15 - Winsock-AFD
    NetEvent ActivityID 16 - Winsock-AFD
    NetEvent ActivityID 17 - TCPIP
    NetEvent ActivityID 18 - Winsock-AFD
    NetEvent ActivityID 19 - Winsock-AFD
    NetEvent ActivityID 20 - Winsock-AFD
    NetEvent ActivityID 21 - Winsock-AFD
    NetEvent ActivityID 22 - TCPIP
    NetEvent ActivityID 23 - Winsock-AFD
    NetEvent ActivityID 24 - Winsock-AFD
    NetEvent ActivityID 25 - TCPIP
    NetEvent ActivityID 26 - TCPIP
    NetEvent ActivityID 27 - Winsock-AFD
    NetEvent ActivityID 28 - TCPIP
    NetEvent ActivityID 29 - Winsock-AFD
    NetEvent ActivityID 30 - TCPIP
    NetEvent ActivityID 31 - Winsock-AFD
    NetEvent ActivityID 32 - Winsock-AFD
    NetEvent ActivityID 33 - Winsock-AFD
    NetEvent ActivityID 34 - TCPIP
    NetEvent ActivityID 35 - TCPIP
    NetEvent ActivityID 36 - TCPIP
    NetEvent ActivityID 37 - TCPIP
    NetEvent ActivityID 38 - TCPIP
    NetEvent ActivityID 39 - TCPIP
    NetEvent ActivityID 40 - TCPIP
    NetEvent ActivityID 41 - Winsock-AFD
    NetEvent ActivityID 42 - Winsock-AFD
```

```
// Show traffic To or From a specific IPv4 address:
//   192.168.0.100 <-> ANY

IPv4.Address == 192.168.72.100

// Show traffic between two IPv4 addresses.  Both addresses
```

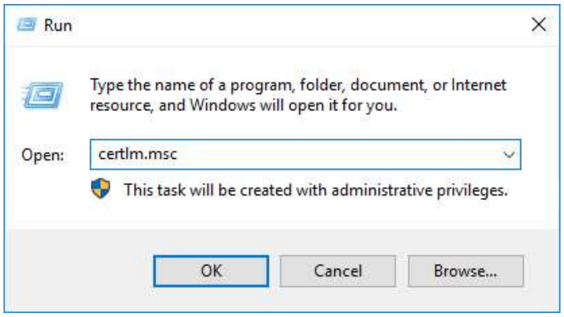
Frame Summary - // Show traffic To or From a specific IPv4 address: //   192.168.0.100 <-> ANY IPv4.Address == 192.168.72.100 // Show traffic between two IPv4 addresses. Both addresses// must be in the packet for it to disp...

```
Frame Number  Time Date Local Adjusted  Time Offset  UT Process Name  Source          Destination     Protocol Name  Description
479           2:44:53 PM 2020-03-04     17.7167133   (4600)           192.168.72.100  192.168.72.10   TCP            TCP: [Bad CheckSum]Flags=......S., SrcPort=57200, DstPort=ldap protocol over TLS/SSL (was sldap)(636), PayloadLen=...
480           2:44:53 PM 2020-03-04     17.7171886   (4)              192.168.72.10   192.168.72.100  TCP            TCP:Flags=...A..S., SrcPort=ldap protocol over TLS/SSL (was sldap)(636), DstPort=57200, PayloadLen=0, Seq=39977...
500           2:44:53 PM 2020-03-04     17.7172889   (4)              192.168.72.100  192.168.72.10   TCP            TCP: [Bad CheckSum]Flags=...A...., SrcPort=57200, DstPort=ldap protocol over TLS/SSL (was sldap)(636), PayloadLen...
519           2:44:53 PM 2020-03-04     17.7205010   (4600)           192.168.72.100  192.168.72.10   TLS            TLS:TLS Rec Layer-1 HandShake: Client Hello.
521           2:44:53 PM 2020-03-04     17.7241800   (0)              192.168.72.10   192.168.72.100  TLS            TLS:TLS Rec Layer-1 HandShake: Server Hello. Certificate.
522           2:44:53 PM 2020-03-04     17.7241820   (0)              192.168.72.10   192.168.72.100  TCP            TCP:[Continuation to #521]Flags=...AP..., SrcPort=ldap protocol over TLS/SSL (was sldap)(636), DstPort=57200, Paylo...
541           2:44:53 PM 2020-03-04     17.7242695   (0)              192.168.72.100  192.168.72.10   TCP            TCP: [Bad CheckSum]Flags=...A...., SrcPort=57200, DstPort=ldap protocol over TLS/SSL (was sldap)(636), PayloadLen...
549           2:44:53 PM 2020-03-04     17.7443722   (4600)           192.168.72.100  192.168.72.10   TLS            TLS:TLS Rec Layer-1 HandShake: Certificate. Client Key Exchange.; TLS Rec Layer-2 Cipher Change Spec; TLS Rec Layer...
551           2:44:53 PM 2020-03-04     17.7459575   (0)              192.168.72.10   192.168.72.100  TLS            TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec Layer-2 HandShake: Encrypted Handshake Message.
567           2:44:53 PM 2020-03-04     17.7643860   (4600)           192.168.72.100  192.168.72.10   LDAP           LDAP:Encrypted Over SSL
570           2:44:53 PM 2020-03-04     17.7650039   (6532)           192.168.72.10   192.168.72.100  LDAP           LDAP:Encrypted Over SSL
571           2:44:53 PM 2020-03-04     17.7650057   (6532)           192.168.72.10   192.168.72.100  TCP            TCP:[Continuation to #570]Flags=...A...., SrcPort=ldap protocol over TLS/SSL (was sldap)(636), DstPort=57200, Paylo...
572           2:44:53 PM 2020-03-04     17.7650072   (6532)           192.168.72.10   192.168.72.100  TCP            TCP:[Continuation to #570]Flags=...AP...., SrcPort=ldap protocol over TLS/SSL (was sldap)(636), DstPort=57200, Paylo...
```

```
Cert: 0x1
  CertLength: 1570 (0x622)
  Certificates:
    CertificateLength: 1567 (0x61F)
    X509Cert: Issuer: TheDroog-THEDROOGDC1-CA,TheDroog,droog, Subject: TheDroogDC1.TheDroog.droog
      SequenceHeader:
      TbsCertificate: Issuer: TheDroog-THEDROOGDC1-CA,TheDroog,droog, Subject: TheDroogDC1.TheDroog.droog
        SequenceHeader:
        Tag0:
        Version: v3 (2)
        SerialNumber: 0x6600000002aabea1ba00a60014000000000002
        Signature: Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
        Issuer: TheDroog-THEDROOGDC1-CA,TheDroog,droog
        Validity: From: 03/04/20 14:52:23 UTC To: 03/04/21 14:52:23 UTC
        Subject: TheDroogDC1.TheDroog.droog
        SubjectPublicKeyInfo: RsaEncryption (1.2.840.113549.1.1.1)
        Tag3:
```

Version 3.4.2350.0   Displayed: 54   Captured: 975   Focused: 521   Selected: 1

6.) On Domain Controller run certlm.msc



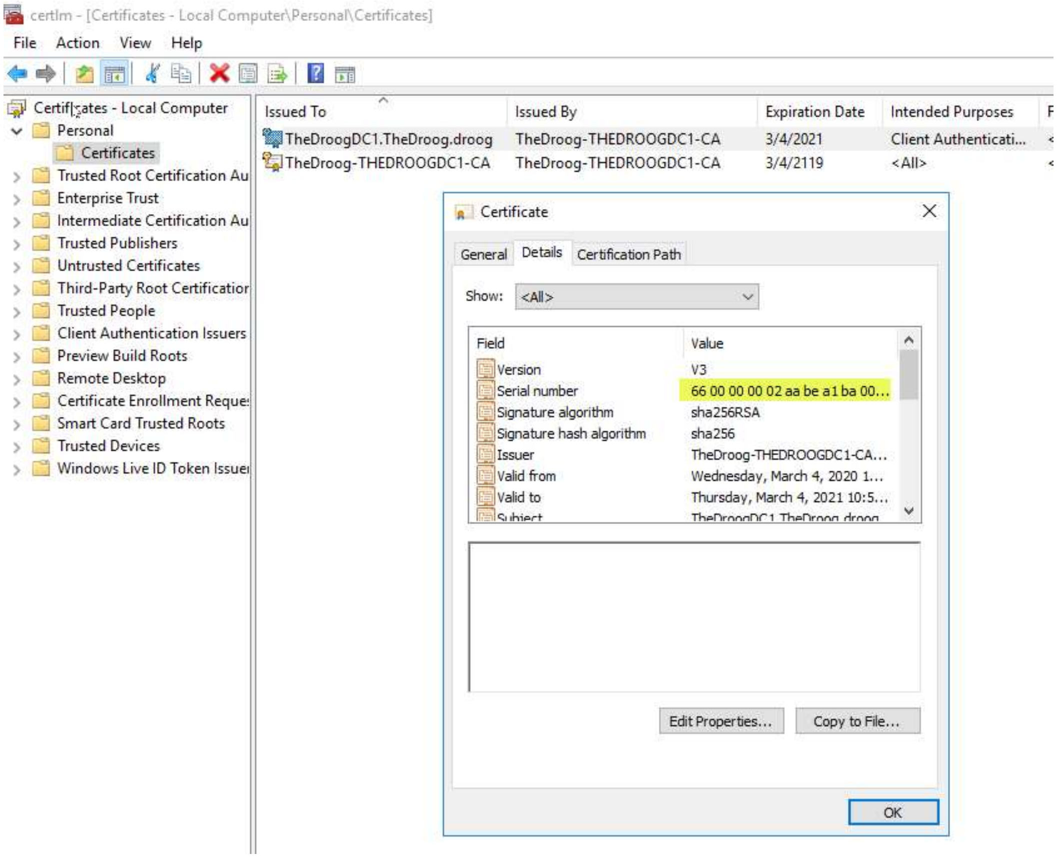
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certlm.msc

This task will be created with administrative privileges.

7.) Browse to Certificates – Local Computer > Personal > Certificates

8.) Double click each certificate > Details Pane and compare the Serial number to what was found in MS Network Monitor 3.4



Issued To	Issued By	Expiration Date	Intended Purposes
TheDroogDC1.TheDroog.droog	TheDroog-THEDROOGDC1-CA	3/4/2021	Client Authenticati...
TheDroog-THEDROOGDC1-CA	TheDroog-THEDROOGDC1-CA	3/4/2119	<All>

Field	Value
Version	V3
Serial number	66 00 00 00 02 aa be a1 ba 00...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	TheDroog-THEDROOGDC1-CA...
Valid from	Wednesday, March 4, 2020 1...
Valid to	Thursday, March 4, 2021 10:5...
Subject	TheDroogDC1.TheDroog.droog

The serial number has been found and definitively shows which certificate is performing the LDAPS authentication.

LDAP over SSL (LDAPS) Certificate
https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

Using ldp.exe
https://www.active-directory-security.com/2016/06/ldp-for-active-directory-download-usage-tutorial-and-examples.html

Microsoft Network Monitor 3.4 download
https://www.microsoft.com/en-ca/download/details.aspx?id=4865

Troubles with Parsers in MS Net Mon 3.4:
https://enblog.alex-trofimov.com/2011/06/20/network-trace-without-netmon-wireshark-etc/