SSE Assignment 2

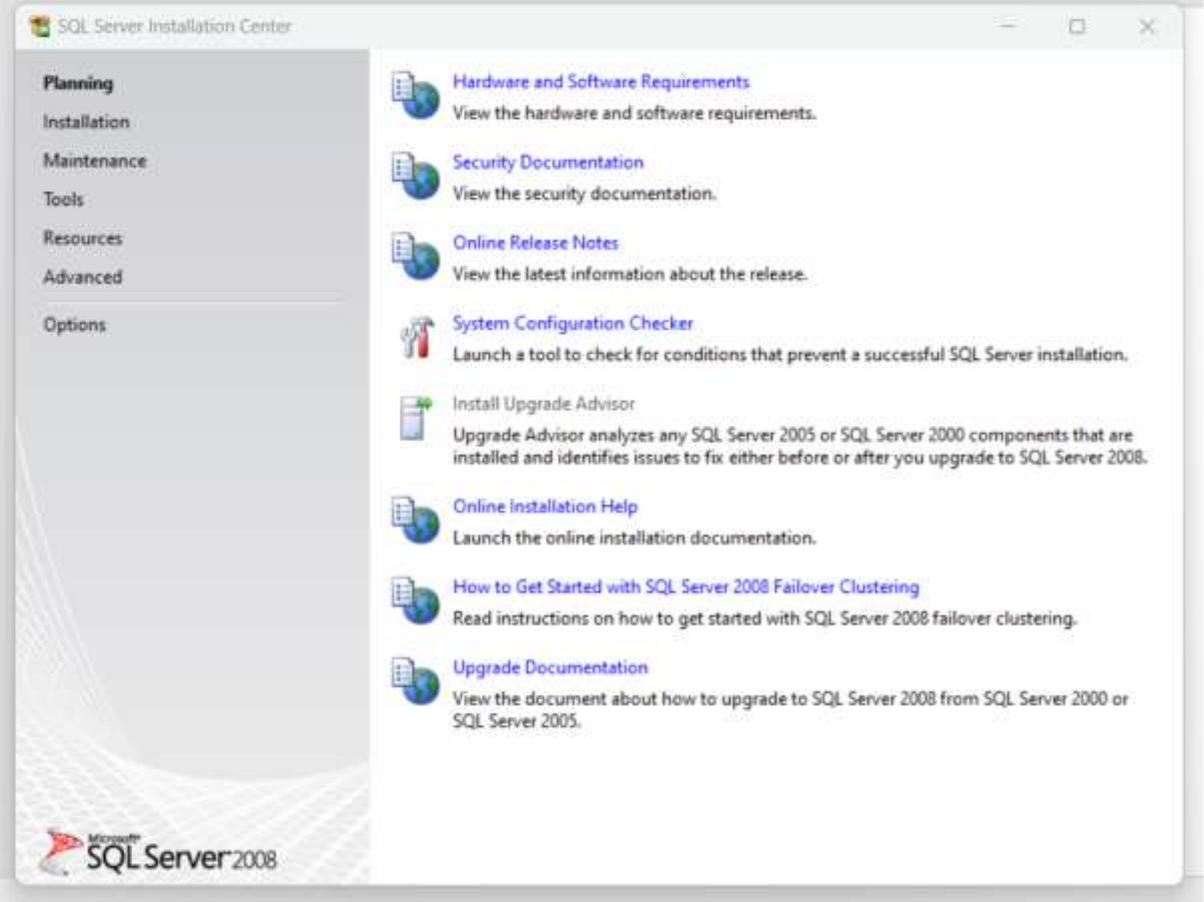
Ananthanarayanan S

CB.SC.P2CYS23007

DVTA Setup - DVTA - Part 1 - Setup (parsiya.net)

Use CFF Framework to analyse custom DVTA.exe created above.

To Start with the DVTA, first we need to setup SQL Server 2008



Hardware and Software Requirements
View the hardware and software requirements.

Security Documentation
View the security documentation.

Online Release Notes
View the latest information about the release.

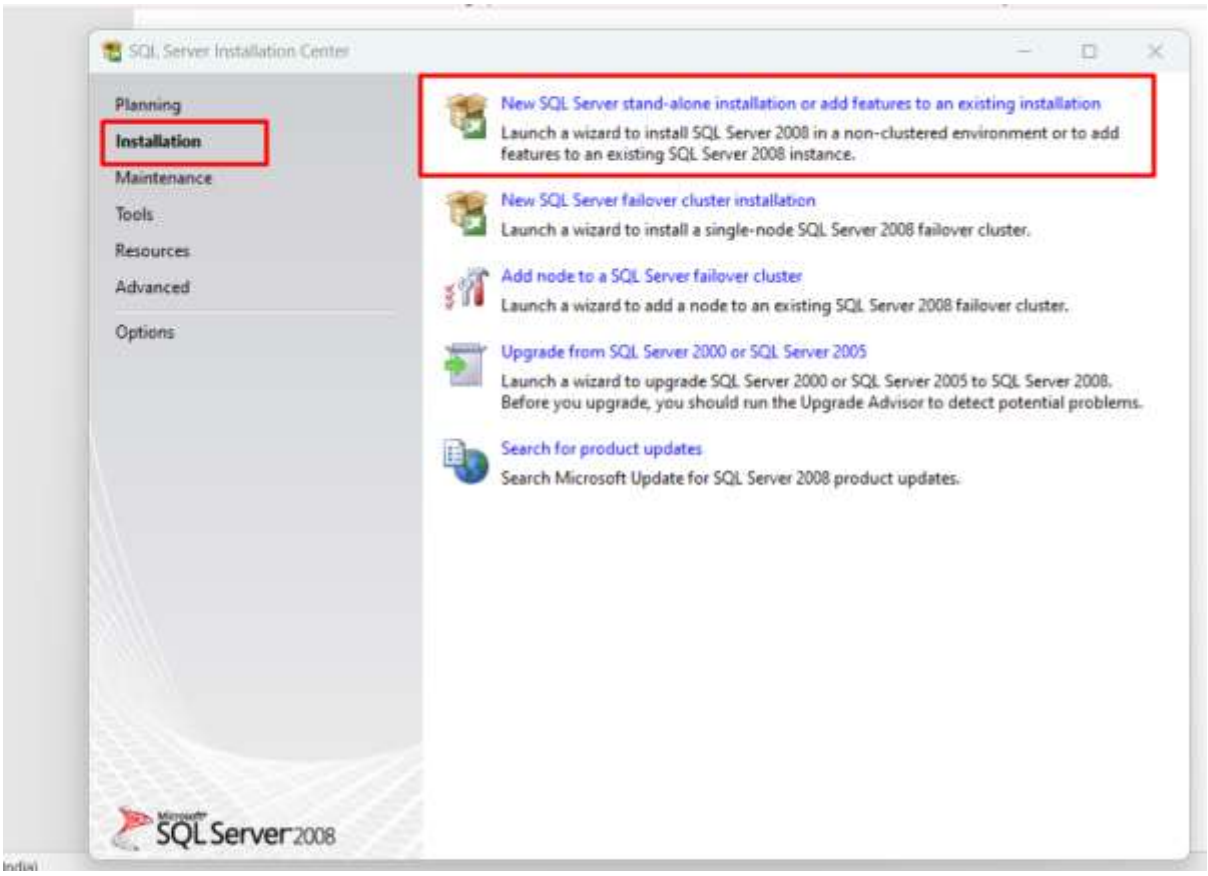
System Configuration Checker
Launch a tool to check for conditions that prevent a successful SQL Server installation.

Install Upgrade Advisor
Upgrade Advisor analyzes any SQL Server 2005 or SQL Server 2000 components that are installed and identifies issues to fix either before or after you upgrade to SQL Server 2008.

Online Installation Help
Launch the online installation documentation.

How to Get Started with SQL Server 2008 Failover Clustering
Read instructions on how to get started with SQL Server 2008 failover clustering.

Upgrade Documentation
View the document about how to upgrade to SQL Server 2008 from SQL Server 2000 or SQL Server 2005.



SQL Server Installation Center

New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2008 in a non-clustered environment or to add features to an existing SQL Server 2008 instance.

New SQL Server failover cluster installation

Launch a wizard to install a single-node SQL Server 2008 failover cluster.

Add node to a SQL Server failover cluster

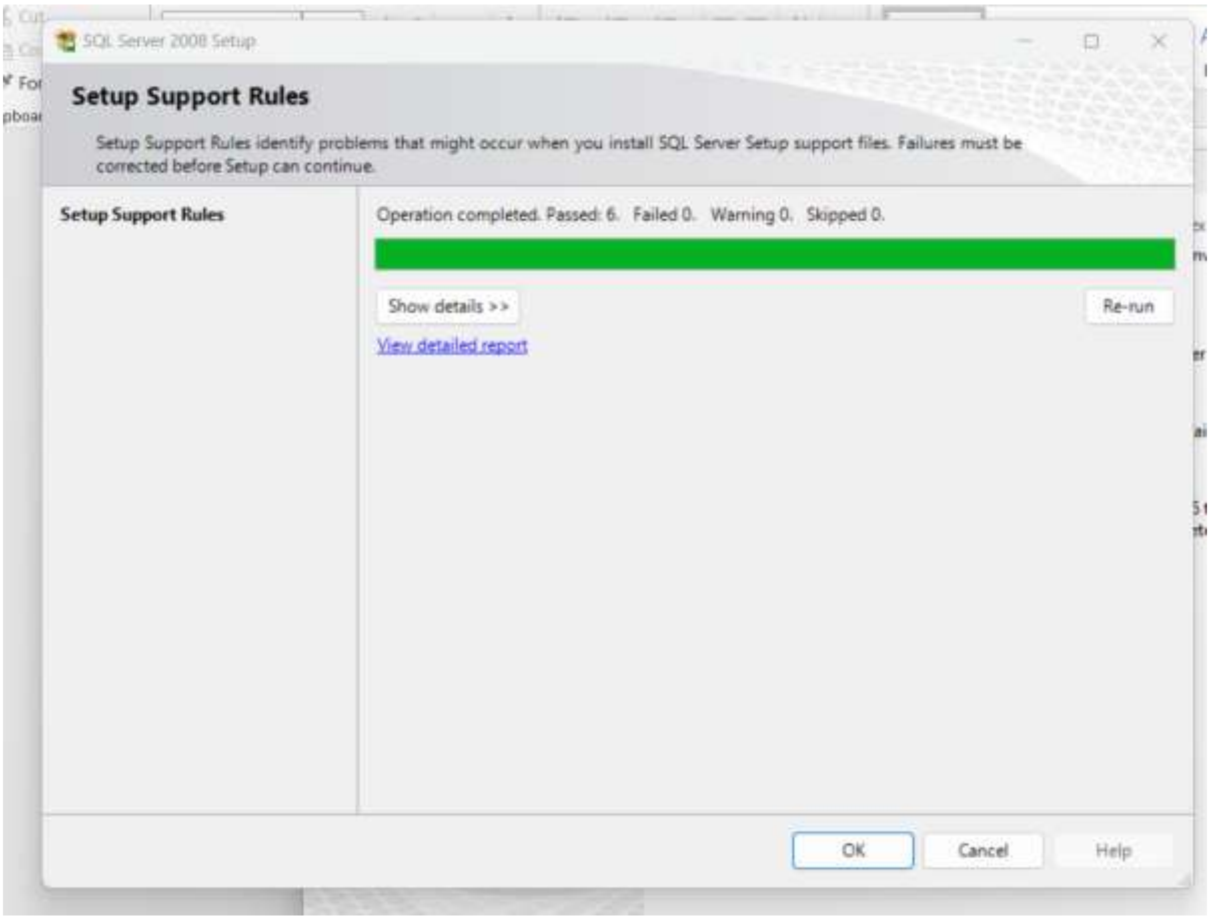
Launch a wizard to add a node to an existing SQL Server 2008 failover cluster.

Upgrade from SQL Server 2000 or SQL Server 2005

Launch a wizard to upgrade SQL Server 2000 or SQL Server 2005 to SQL Server 2008. Before you upgrade, you should run the Upgrade Advisor to detect potential problems.

Search for product updates

Search Microsoft Update for SQL Server 2008 product updates.



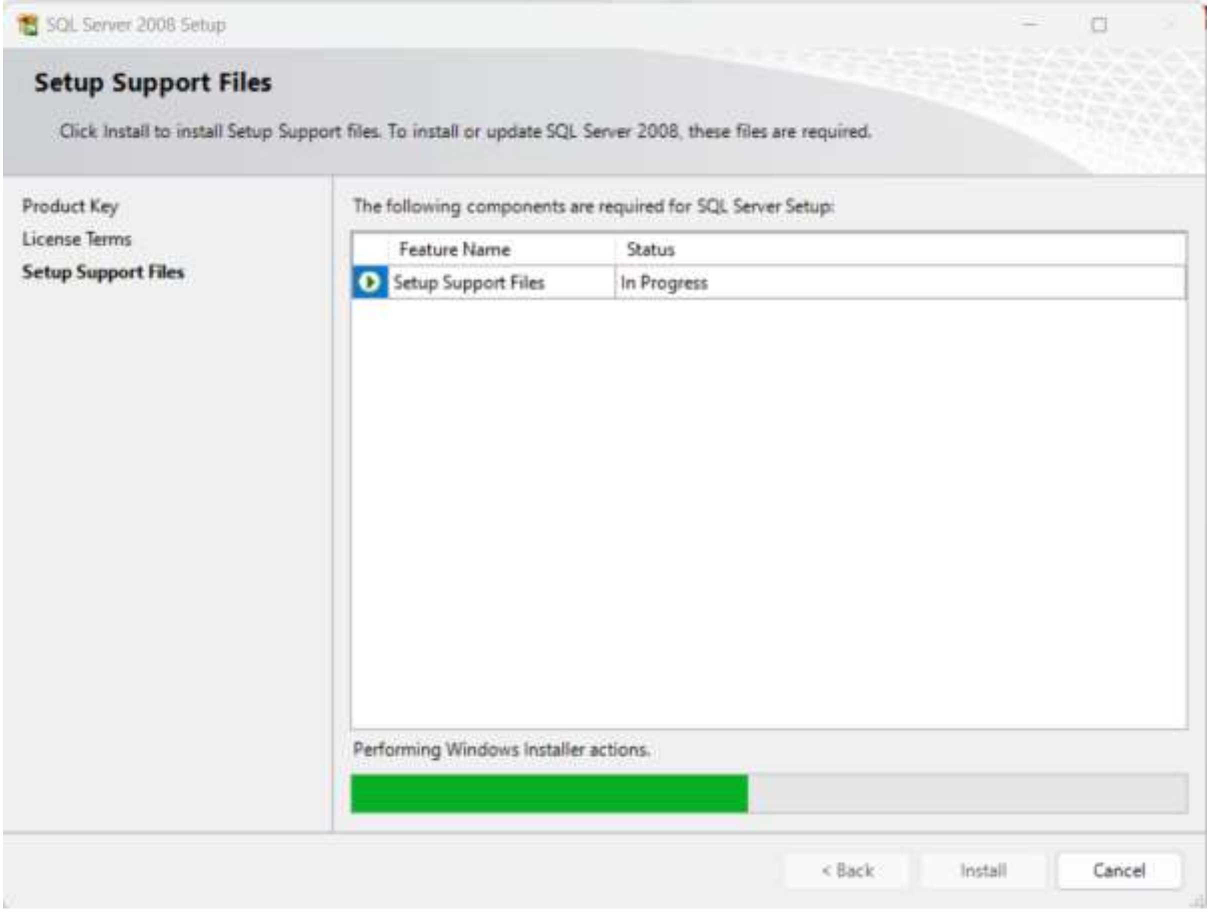
SQL Server 2008 Setup

Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Operation completed. Passed: 6. Failed 0. Warning 0. Skipped 0.

We have to setup support files



SQL Server 2008 Setup

Setup Support Files

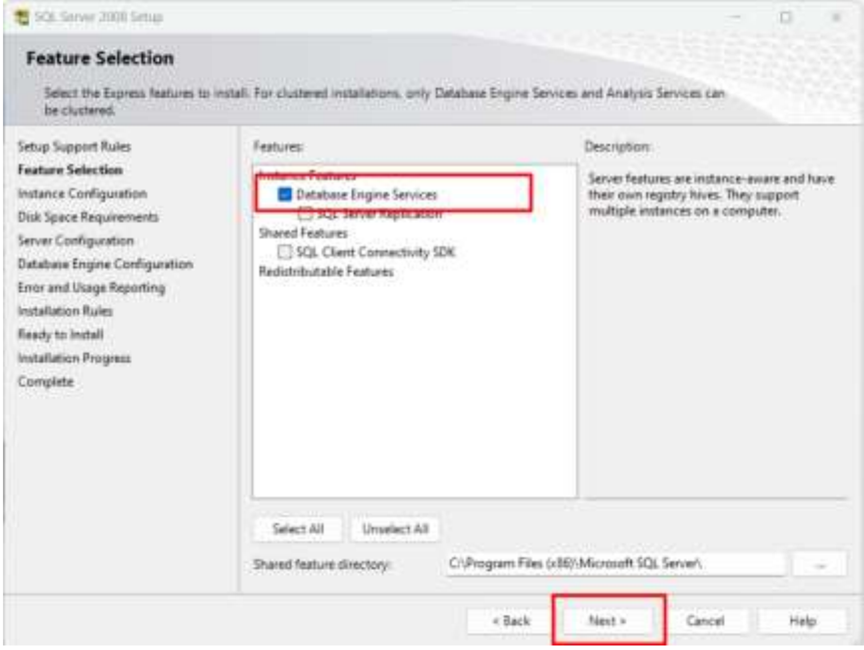
Click Install to install Setup Support files. To install or update SQL Server 2008, these files are required.

The following components are required for SQL Server Setup:

Feature Name	Status
Setup Support Files	In Progress

Performing Windows Installer actions.

Add Database Engine



SQL Server 2008 Setup

Feature Selection

Select the Express features to install. For clustered installations, only Database Engine Services and Analysis Services can be clustered.

Features:

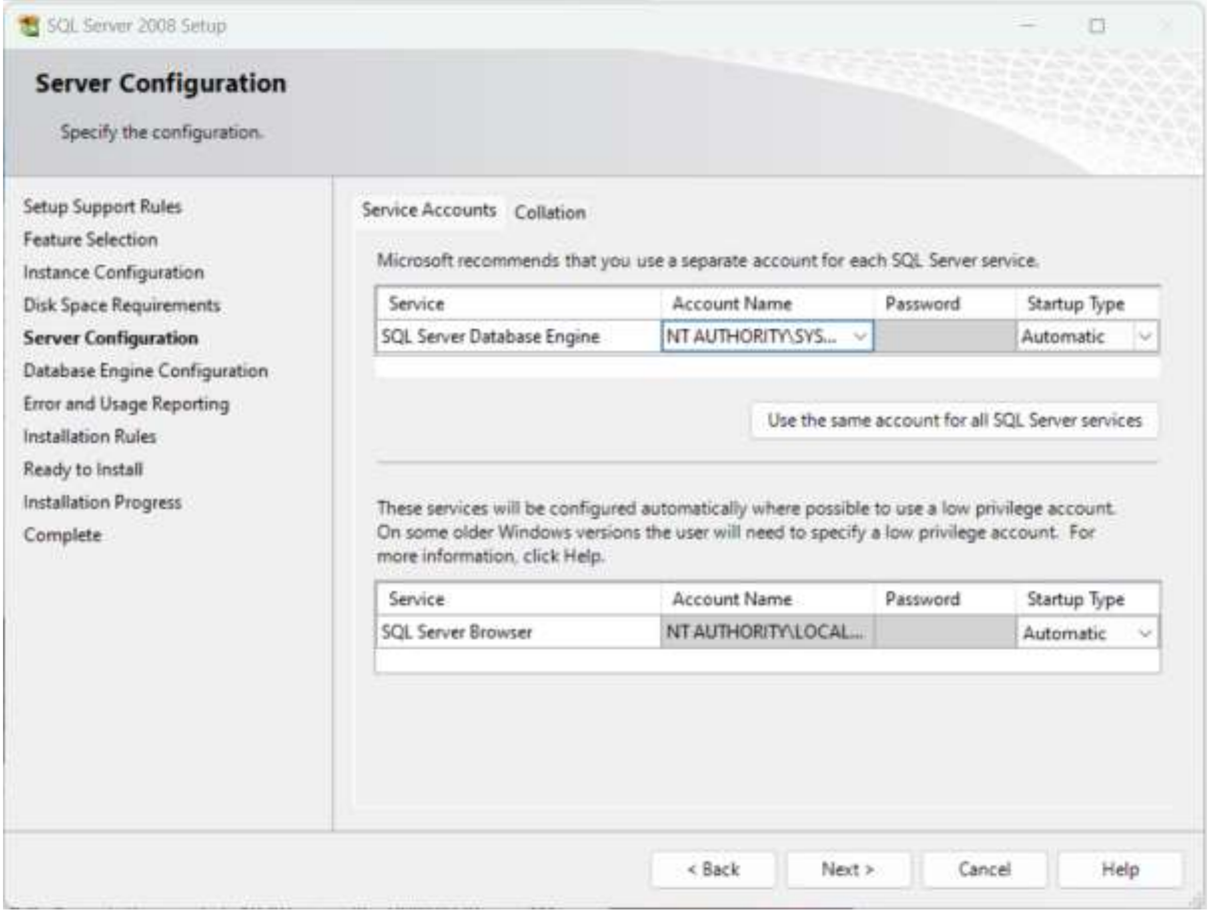
Instance Features
☑ Database Engine Services
□ SQL Server Replication
Shared Features
□ SQL Client Connectivity SDK
Redistributable Features

Description:

Server features are instance-aware and have their own registry hives. They support multiple instances on a computer.

Shared feature directory: C:\Program Files (x86)\Microsoft SQL Server\

Now configure server



Server Configuration

Specify the configuration.

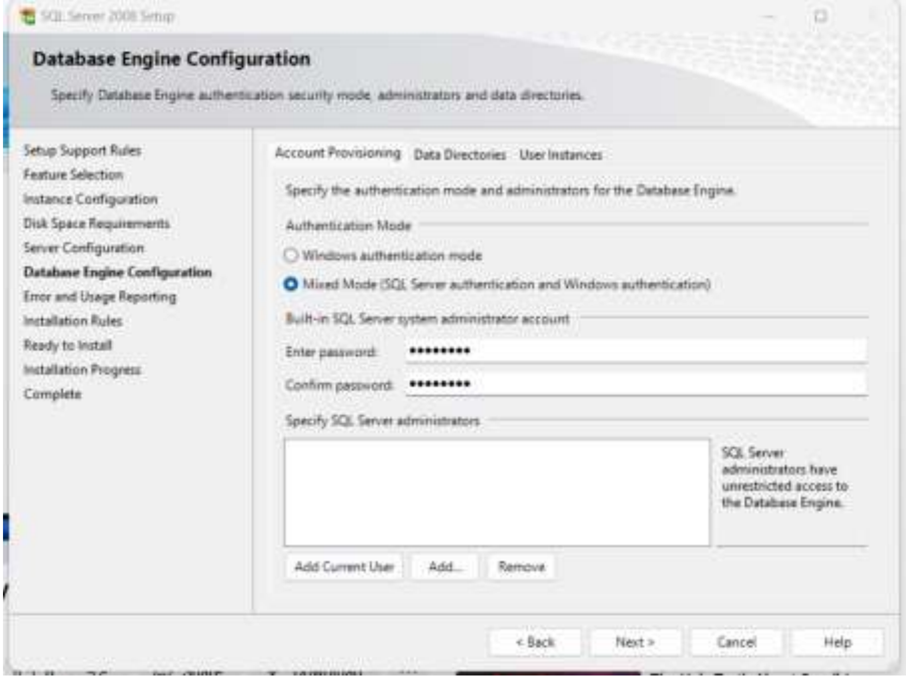
Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT AUTHORITY\SYS...		Automatic

These services will be configured automatically where possible to use a low privilege account. On some older Windows versions the user will need to specify a low privilege account. For more information, click Help.

Service	Account Name	Password	Startup Type
SQL Server Browser	NT AUTHORITY\LOCAL...		Automatic

Add a password as a configuration of Server



Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

Enter password: *********

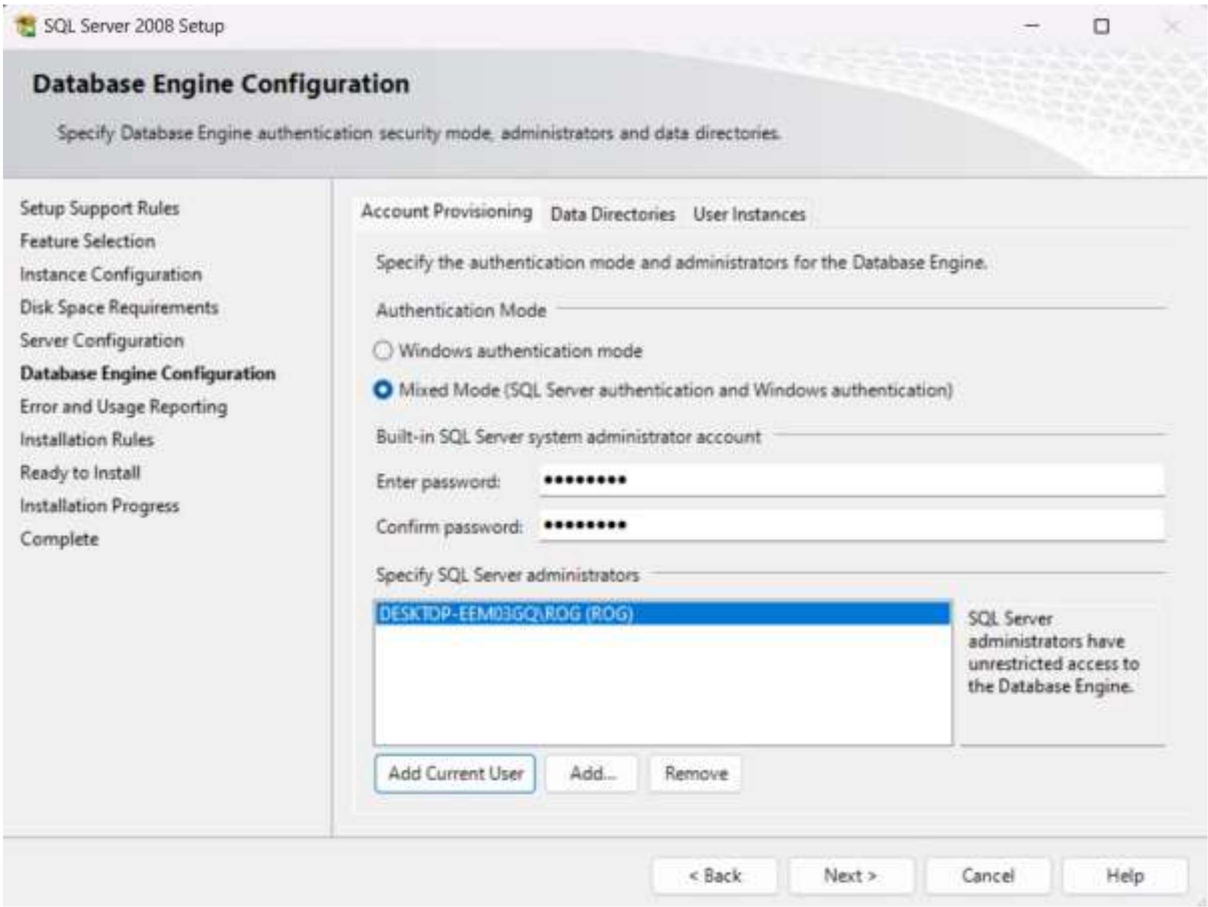
Confirm password: *********

Specify SQL Server administrators

SQL Server administrators have unrestricted access to the Database Engine.

Password Should be – 12345678

- We need to add users SQL Server Administrator



Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

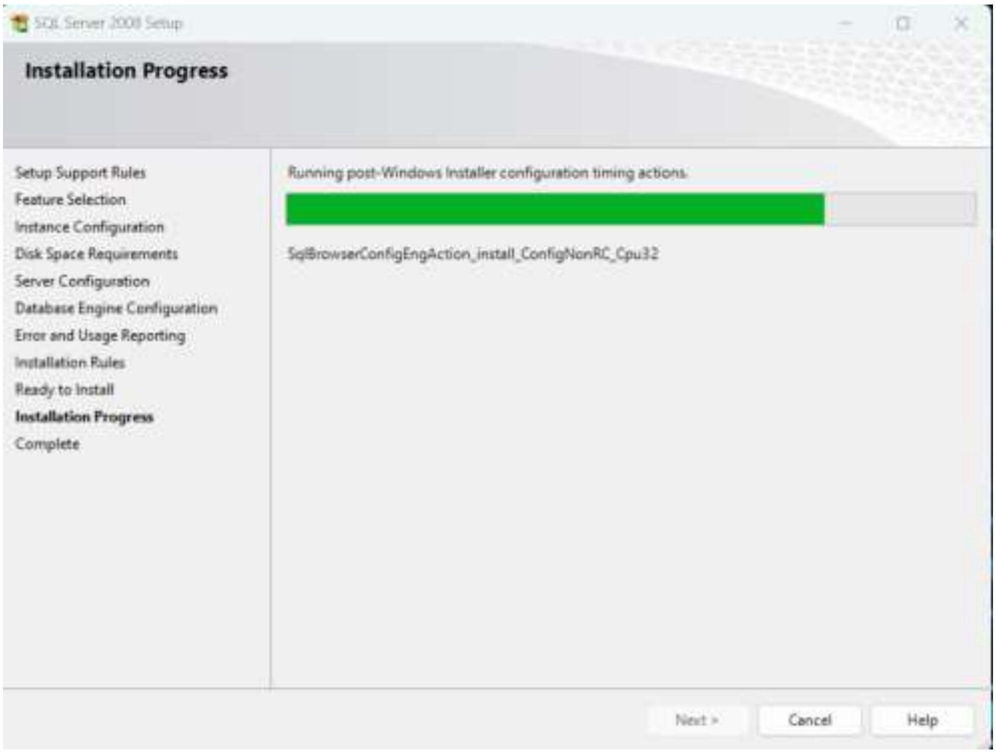
Enter password: ••••••••

Confirm password: ••••••••

Specify SQL Server administrators

DESKTOP-EEM03GQ\ROG (ROG)

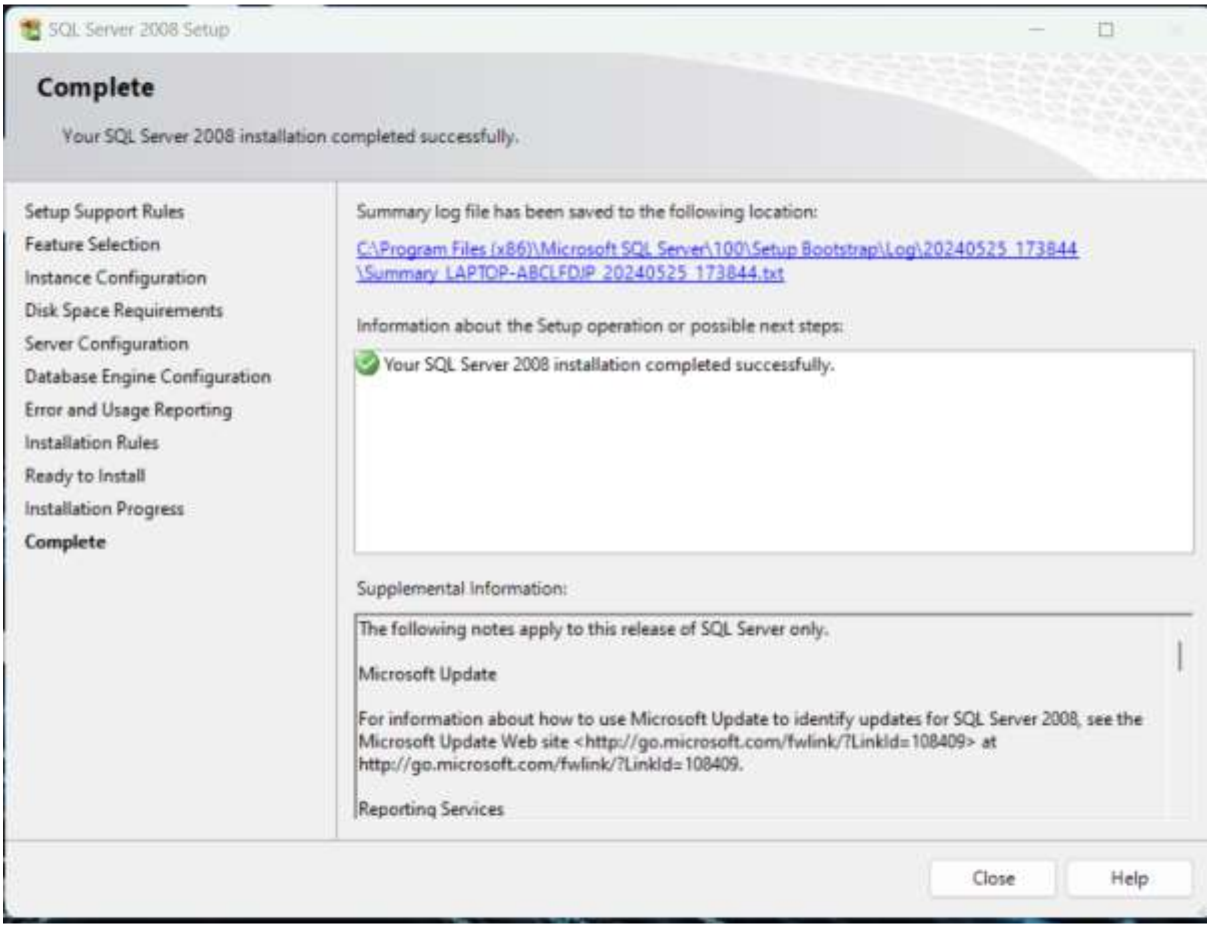
SQL Server administrators have unrestricted access to the Database Engine.



Installation Progress

Running post-Windows Installer configuration timing actions.

SqlBrowserConfigEngAction_install_ConfigNonRC_Cpu32



Complete

Your SQL Server 2008 installation completed successfully.

Summary log file has been saved to the following location:

C:\Program Files (x86)\Microsoft SQL Server\100\Setup Bootstrap\Log\20240525_173844
\Summary_LAPTOP-ABCLFDJP_20240525_173844.txt

Information about the Setup operation or possible next steps:

✓ Your SQL Server 2008 installation completed successfully.

Supplemental Information:

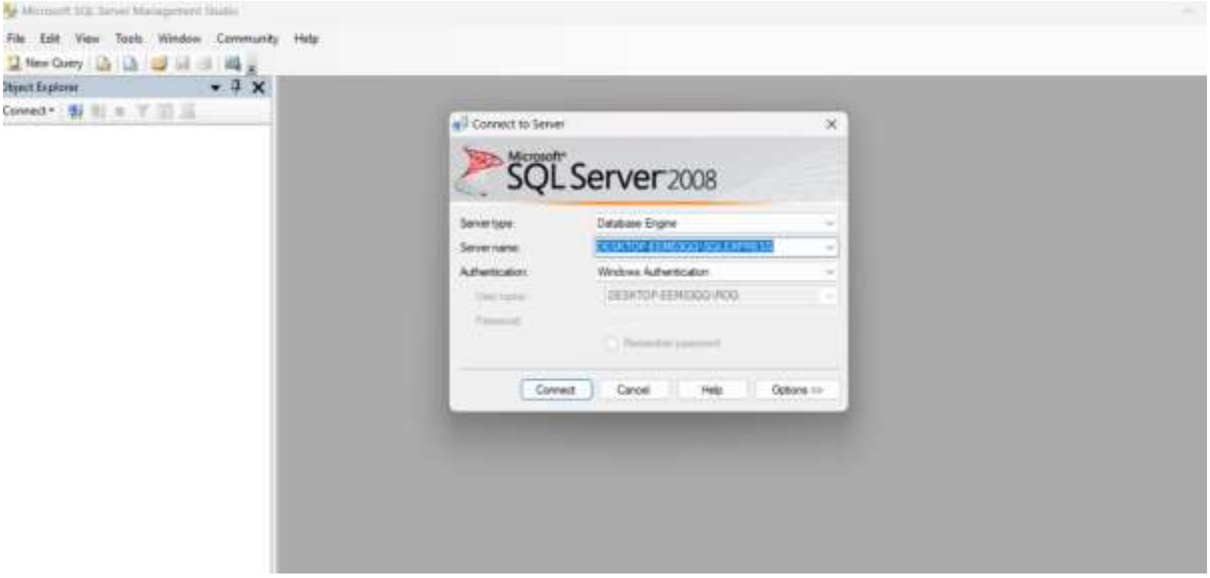
The following notes apply to this release of SQL Server only.

Microsoft Update

For information about how to use Microsoft Update to identify updates for SQL Server 2008, see the Microsoft Update Web site <http://go.microsoft.com/fwlink/?LinkId=108409> at http://go.microsoft.com/fwlink/?LinkId=108409.

Reporting Services

- start SQL Server 2008



Server type: Database Engine

Server name: DESKTOP-EEMI0QQ\SQLEXPRESS

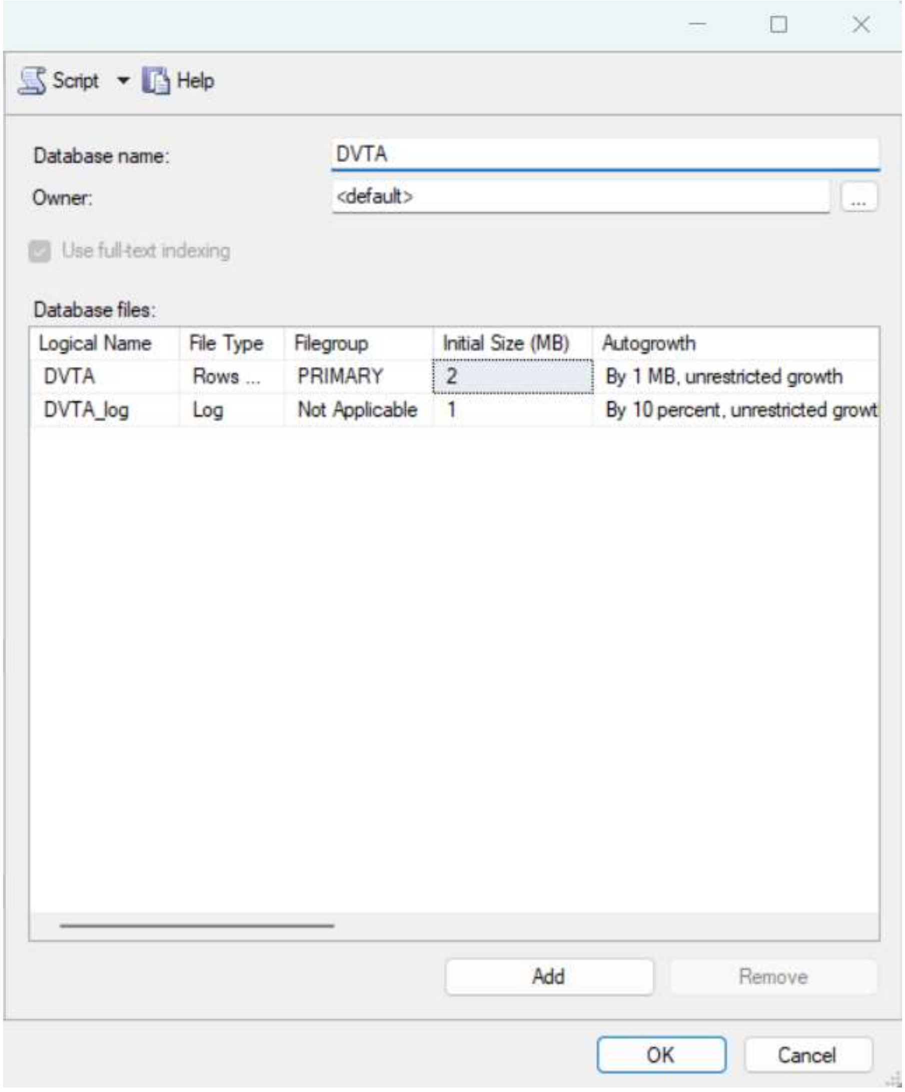
Authentication: Windows Authentication

User name: DESKTOP-EEMI0QQ\ROO

Password:

□ Remember password

Create New Database



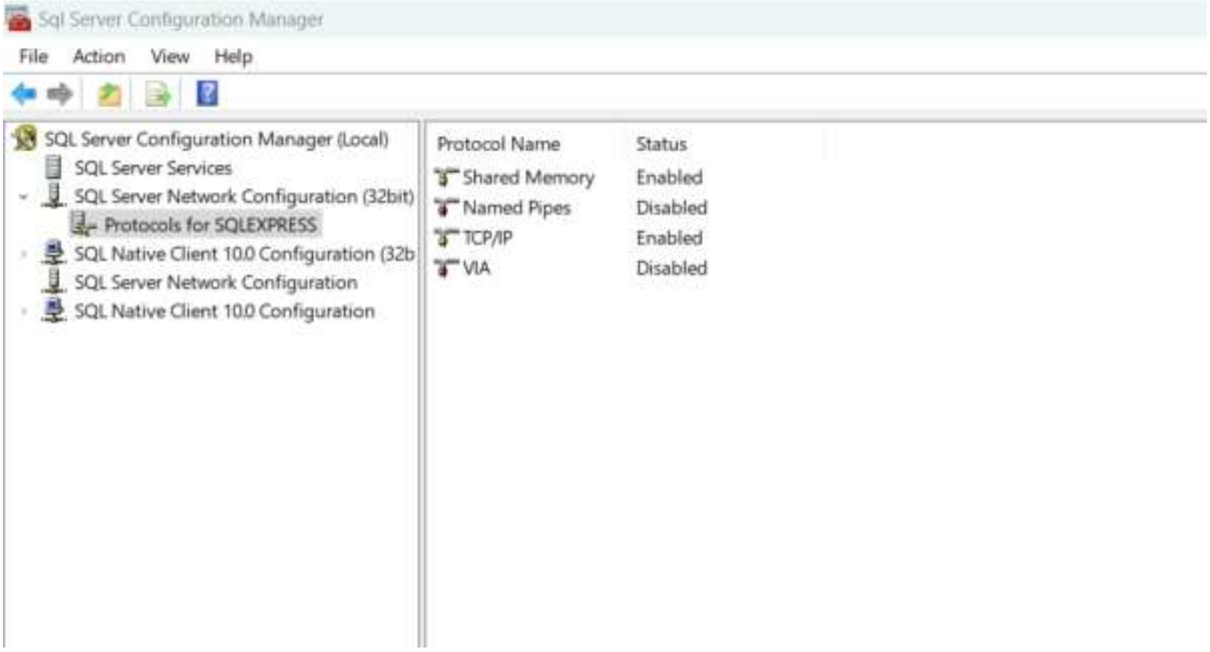
Database name: DVTA

Owner: <default>

☑ Use full-text indexing

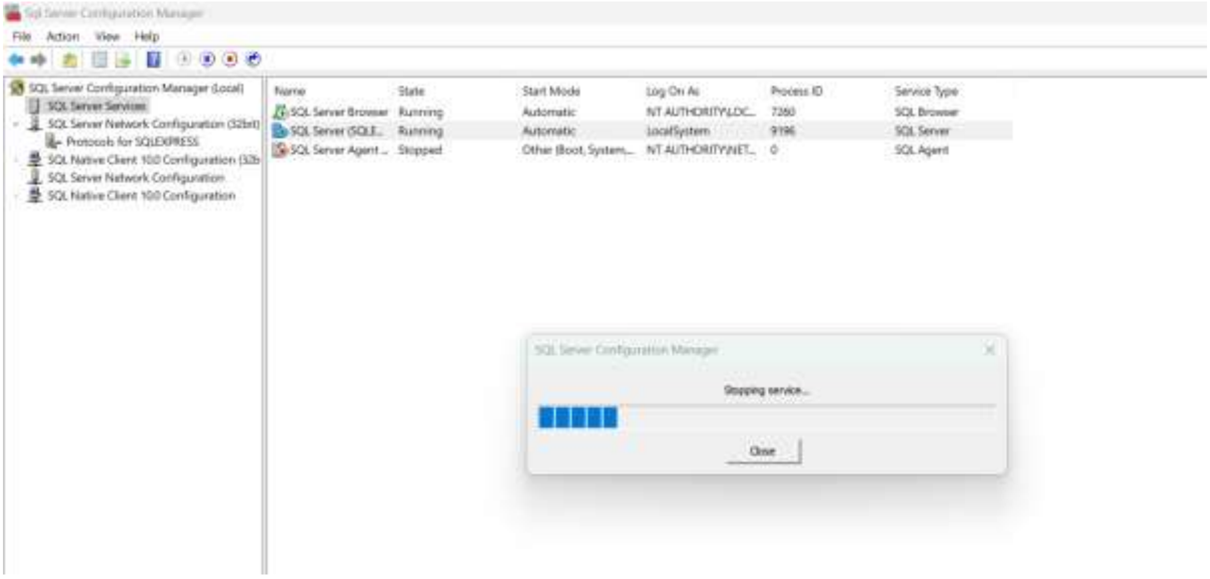
Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth
DVTA	Rows ...	PRIMARY	2	By 1 MB, unrestricted growth
DVTA_log	Log	Not Applicable	1	By 10 percent, unrestricted growt


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration (32b
SQL Server Network Configuration
SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled
VIA	Disabled

- Restart SQL Server

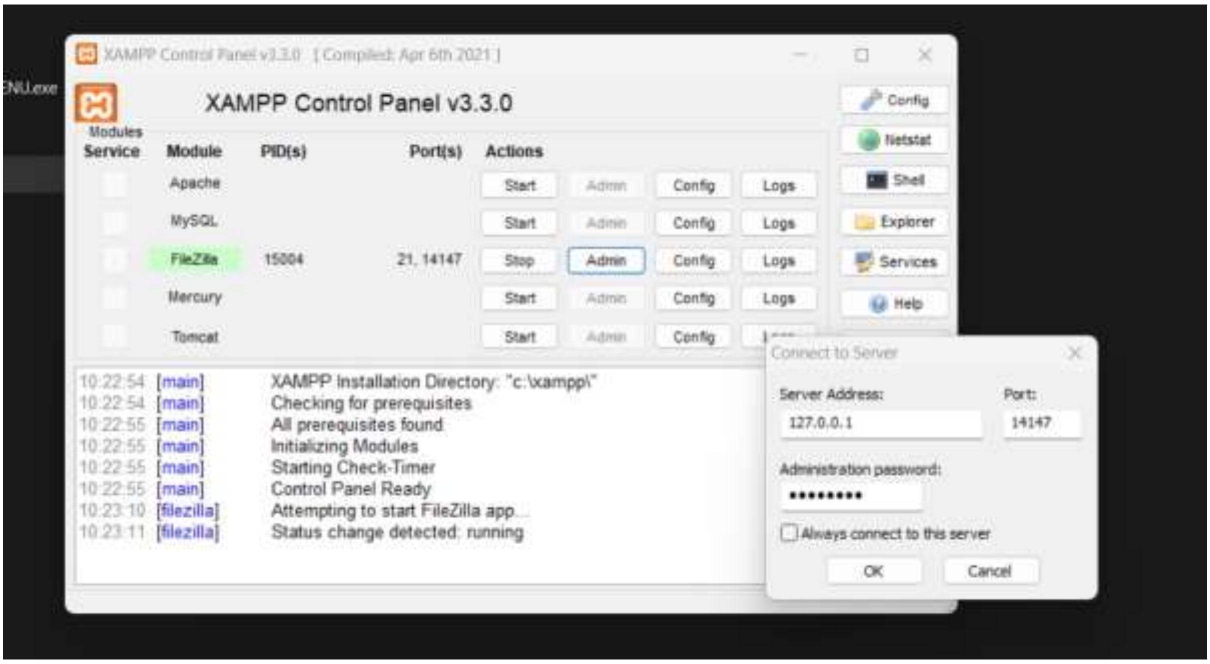


SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration (32b
SQL Server Network Configuration
SQL Native Client 10.0 Configuration

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server Browser	Running	Automatic	NT AUTHORITY\LOC...	7260	SQL Browser
SQL Server (SQLE...	Running	Automatic	LocalSystem	9196	SQL Server
SQL Server Agent ...	Stopped	Other (Boot, System,...	NT AUTHORITY\NET...	0	SQL Agent

SQL Server Configuration Manager

Stopping service...

- Start a Filezila Server in your computer
- Going to Admin Panel
- 

ENU.exe
XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]
XAMPP Control Panel v3.3.0
Config
Netstat
Shell
Explorer
Services
Help

Modules Service	Module	PID(s)	Port(s)	Actions			
	Apache			Start	Admin	Config	Logs
	MySQL			Start	Admin	Config	Logs
	FileZilla	15004	21, 14147	Stop	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
10:22:54  [main]      XAMPP Installation Directory: "c:\xampp\"
10:22:54  [main]      Checking for prerequisites
10:22:55  [main]      All prerequisites found
10:22:55  [main]      Initializing Modules
10:22:55  [main]      Starting Check-Timer
10:22:55  [main]      Control Panel Ready
10:23:10  [filezilla] Attempting to start FileZilla app...
10:23:11  [filezilla] Status change detected: running
```

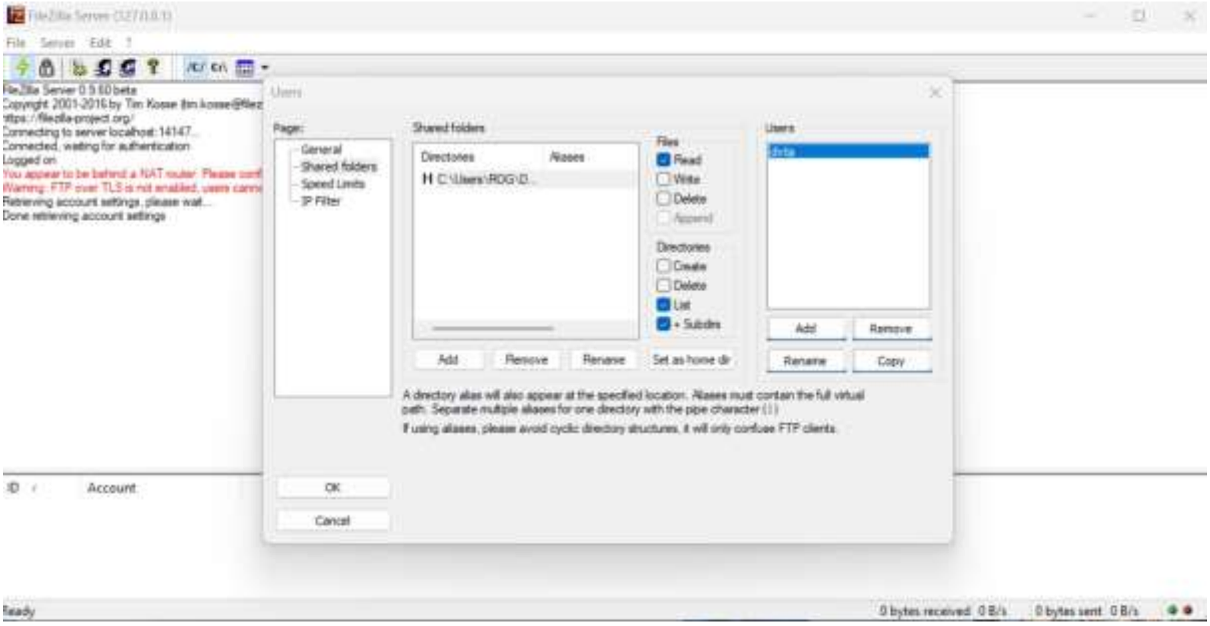
Connect to Server

Server Address: 127.0.0.1

Port: 14147

Administration password: ••••••••

☐ Always connect to this server



```
FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filez
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please conf
Warning: FTP over TLS is not enabled, users cann
Retrieving account settings, please wait...
Done retrieving account settings
```

H C:\Users\ROG\D...

Files
☑ Read
□ Write
□ Delete
□ Append

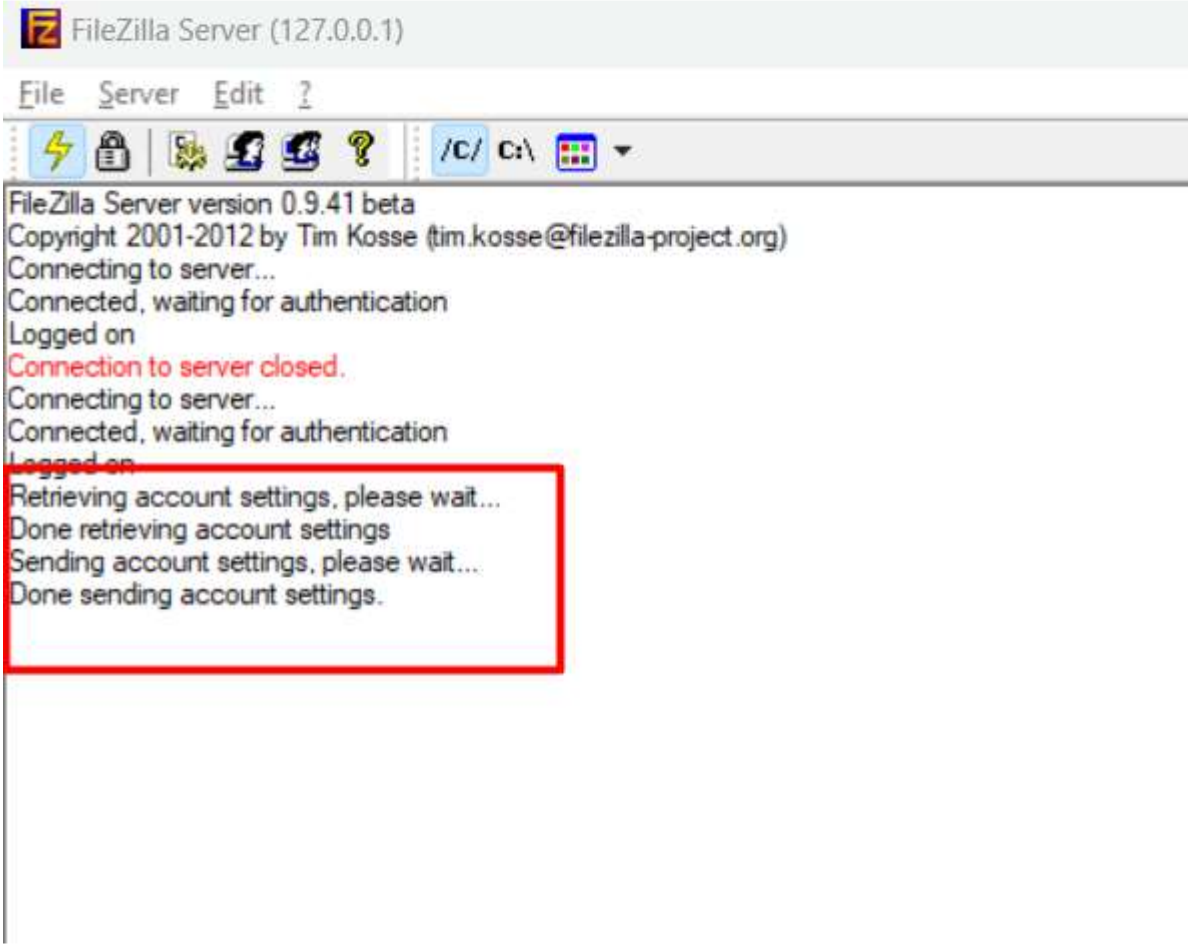
Directories
□ Create
□ Delete
☑ List
☑ + Subdirs

Users: dvta

A directory alias will also appear at the specified location. Aliases must contain the full virtual path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.

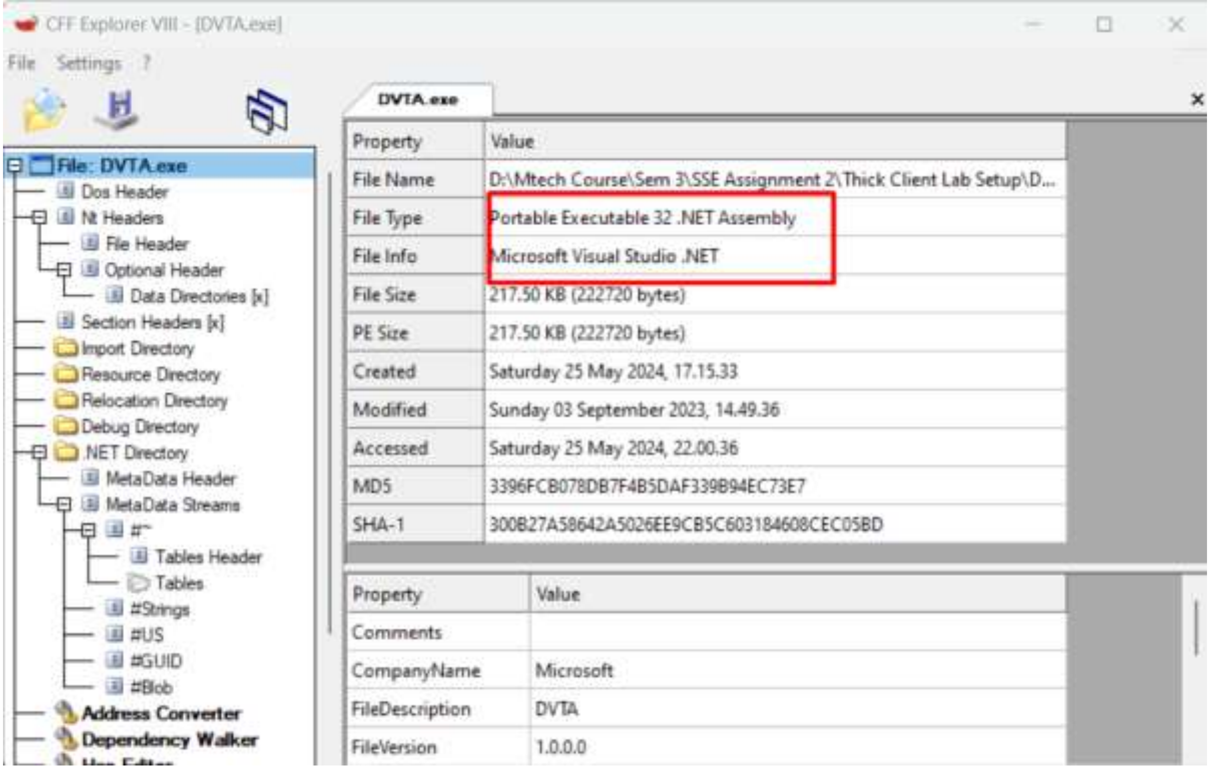
0 bytes received 0 B/s 0 bytes sent 0 B/s



```
FileZilla Server version 0.9.41 beta
Copyright 2001-2012 by Tim Kosse (tim.kosse@filezilla-project.org)
Connecting to server...
Connected, waiting for authentication
Logged on
Connection to server closed.
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving account settings, please wait...
Done retrieving account settings
Sending account settings, please wait...
Done sending account settings.
```

1) Identify the Application architecture, languages and frameworks used?

- Upon opening the dvta.exe in CFF-explorer, we can identify the following information
- Architecture – 32 bit & 2 tier [Since it communicates with the database.]
- Languages used - .NET Assembly
- Frameworks - .NET framework

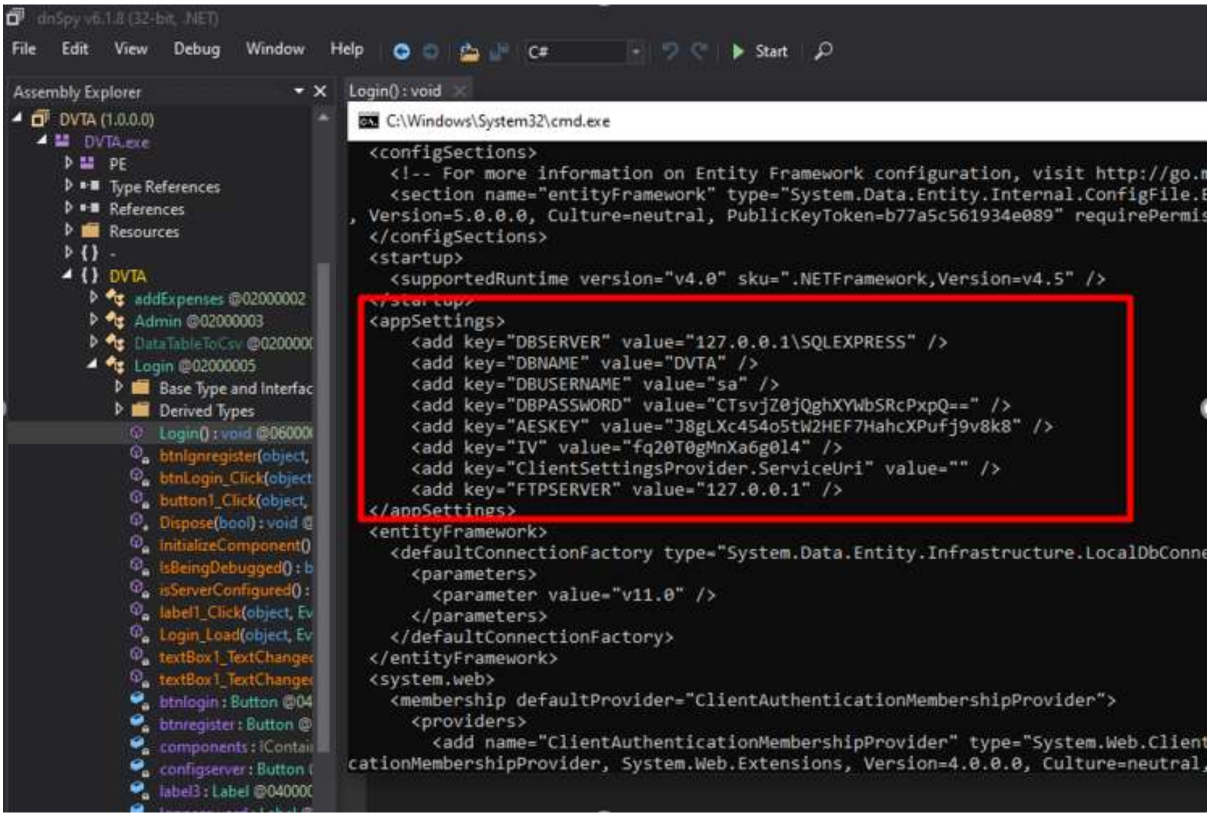


Property	Value
File Name	D:\Mtech Course\Sem 3\SSE Assignment 2\Thick Client Lab Setup\D...
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	217.50 KB (222720 bytes)
PE Size	217.50 KB (222720 bytes)
Created	Saturday 25 May 2024, 17.15.33
Modified	Sunday 03 September 2023, 14.49.36
Accessed	Saturday 25 May 2024, 22.00.36
MD5	3396FCB078DB7F4B5DAF339B94EC73E7
SHA-1	300B27A58642A5026EE9CB5C603184608CEC05BD

Property	Value
Comments	
CompanyName	Microsoft
FileDescription	DVTA
FileVersion	1.0.0.0

2. Decompile and try to retrieve the source code of the application? Also, check if any hardcoded sensitive information is found?

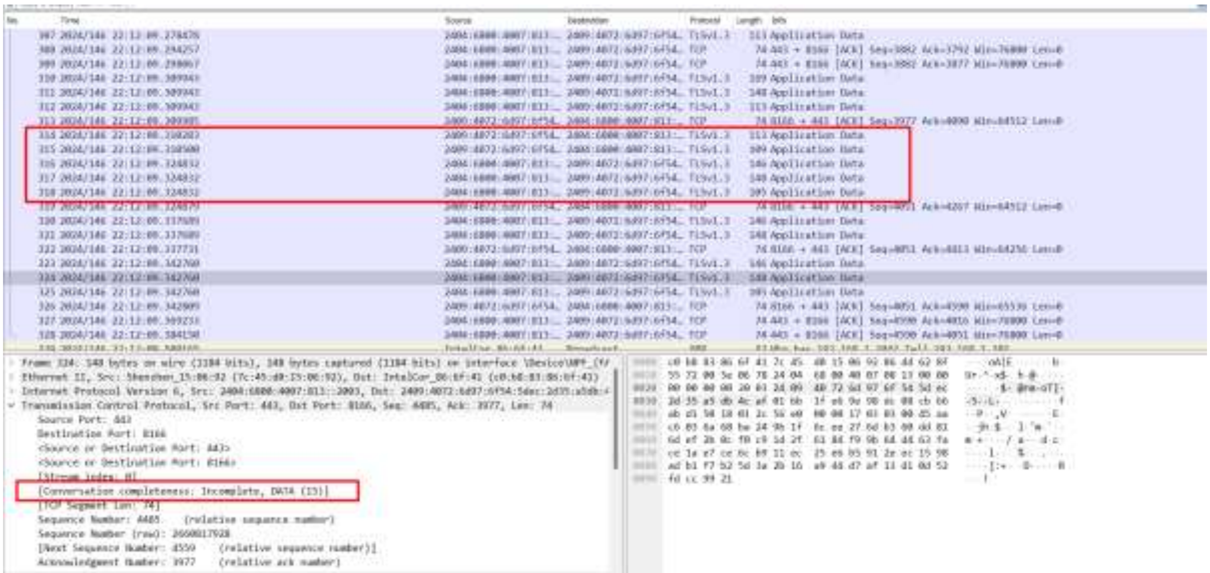
- By decompiling the application using DNSpy or MS Visual studio tools, we can see the source code of the application.



```
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.m
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.E
, Version=5.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermis
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <appSettings>
      <add key="DBSERVER" value="127.0.0.1\SQLEXPRESS" />
      <add key="DBNAME" value="DVTA" />
      <add key="DBUSERNAME" value="sa" />
      <add key="DBPASSWORD" value="CTsvjZ0jQghXYWbSRcPxpQ==" />
      <add key="AESKEY" value="J8gLXc454o5tW2HEF7HahcXPufj9v8k8" />
      <add key="IV" value="fq20T0gMnXa6g0l4" />
      <add key="ClientSettingsProvider.ServiceUri" value="" />
      <add key="FTPSERVER" value="127.0.0.1" />
  </appSettings>
  <entityFramework>
    <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConne
      <parameters>
        <parameter value="v11.0" />
      </parameters>
    </defaultConnectionFactory>
  </entityFramework>
  <system.web>
    <membership defaultProvider="ClientAuthenticationMembershipProvider">
      <providers>
        <add name="ClientAuthenticationMembershipProvider" type="System.Web.Client
cationMembershipProvider, System.Web.Extensions, Version=4.0.0.0, Culture=neutral,
```

3) Sniff the traffic between client and server. Identify which protocol is being used for communication?

- With Wireshark we can sniff the client and server
- Next inspect the contents of the packets to determine whether the app is using TCP/UDP protocol for communication.
- In the packet inspection window, we can see that the protocol used by the dvta is TCP protocol.



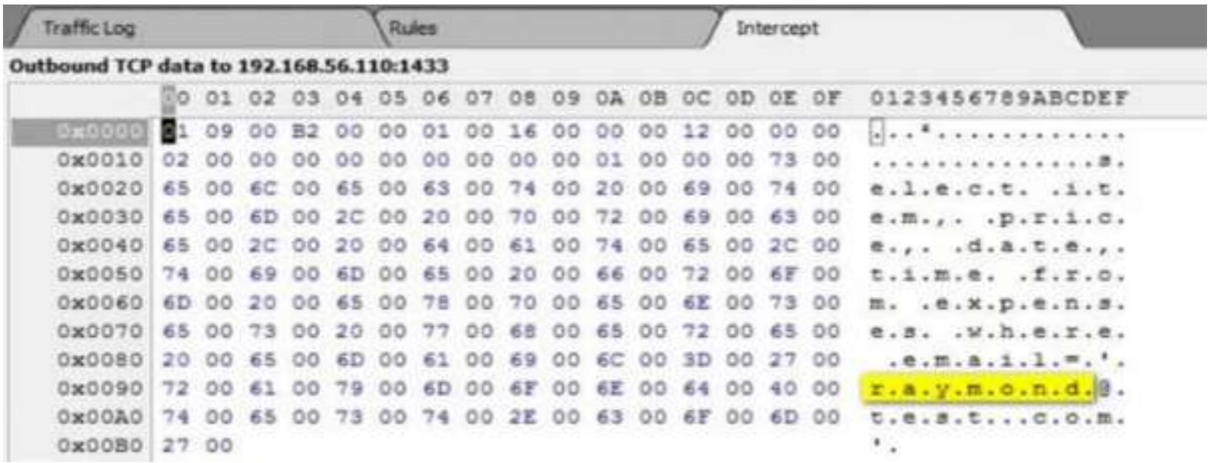
```
307 2024/146 22:12:09.278476   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  113 Application Data
308 2024/146 22:12:09.294257   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TCP       74 443 → 8166 [ACK] Seq=3882 Ack=3792 Win=76800 Len=0
309 2024/146 22:12:09.298067   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TCP       74 443 → 8166 [ACK] Seq=3882 Ack=3877 Win=76800 Len=0
310 2024/146 22:12:09.309943   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  109 Application Data
311 2024/146 22:12:09.309943   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  148 Application Data
312 2024/146 22:12:09.309943   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  113 Application Data
313 2024/146 22:12:09.309985   2409:4072:6d97:6f54…  2404:6800:4007:813:…  TCP       74 8166 → 443 [ACK] Seq=3977 Ack=4090 Win=64512 Len=0
314 2024/146 22:12:09.310203   2409:4072:6d97:6f54…  2404:6800:4007:813:…  TLSv1.3  113 Application Data
315 2024/146 22:12:09.310500   2409:4072:6d97:6f54…  2404:6800:4007:813:…  TLSv1.3  109 Application Data
316 2024/146 22:12:09.324832   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  146 Application Data
317 2024/146 22:12:09.324832   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  148 Application Data
318 2024/146 22:12:09.324832   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  395 Application Data
319 2024/146 22:12:09.324879   2409:4072:6d97:6f54…  2404:6800:4007:813:…  TCP       74 8166 → 443 [ACK] Seq=4051 Ack=4207 Win=64512 Len=0
320 2024/146 22:12:09.337689   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  140 Application Data
321 2024/146 22:12:09.337689   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  148 Application Data
322 2024/146 22:12:09.337731   2409:4072:6d97:6f54…  2404:6800:4007:813:…  TCP       74 8166 → 443 [ACK] Seq=4051 Ack=4413 Win=64256 Len=0
323 2024/146 22:12:09.342760   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  146 Application Data
324 2024/146 22:12:09.342760   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  148 Application Data
325 2024/146 22:12:09.342760   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TLSv1.3  395 Application Data
326 2024/146 22:12:09.342909   2409:4072:6d97:6f54…  2404:6800:4007:813:…  TCP       74 8166 → 443 [ACK] Seq=4051 Ack=4598 Win=65536 Len=0
327 2024/146 22:12:09.369231   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TCP       74 443 → 8166 [ACK] Seq=4598 Ack=4016 Win=76800 Len=0
328 2024/146 22:12:09.384158   2404:6800:4007:813:…  2409:4072:6d97:6f54…  TCP       74 443 → 8166 [ACK] Seq=4598 Ack=4051 Win=76800 Len=0
```

```
> Frame 324: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface \Device\NPF_{F/
> Ethernet II, Src: Shenzhen_15:06:92 (7c:45:d0:15:06:92), Dst: IntelCor_86:6f:41 (c0:b6:83:86:6f:41)
> Internet Protocol Version 6, Src: 2404:6800:4007:813::2003, Dst: 2409:4072:6d97:6f54:5dec:2d35:a5db:4
v Transmission Control Protocol, Src Port: 443, Dst Port: 8166, Seq: 4485, Ack: 3977, Len: 74
    Source Port: 443
    Destination Port: 8166
    <Source or Destination Port: 443>
    <Source or Destination Port: 8166>
    [Stream index: 8]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 74]
    Sequence Number: 4485    (relative sequence number)
    Sequence Number (raw): 2660017928
    [Next Sequence Number: 4559    (relative sequence number)]
    Acknowledgment Number: 3977    (relative ack number)
```

```
0000  c0 b6 83 86 6f 41 7c 45 d0 15 06 92 86 dd 62 8f
0010  55 72 00 5c 06 78 24 04 68 00 40 07 08 13 00 00
0020  00 00 00 00 20 03 24 09 40 72 6d 97 6f 54 5d ec
0030  2d 35 a5 db 4c af 01 bb 1f e6 9e 98 ec 08 cb 06
0040  ab d1 58 18 01 2c 56 a0 00 00 17 01 03 00 45 aa
0050  c6 03 6a 68 be 24 9b 1f 8c ee 27 6d b3 00 dd 83
0060  6d ef 2b 8c f0 c9 5d 2f 61 8d f9 9b 6d 44 62 fa
0070  ce 1a e7 ce 8c b9 11 ec 25 e6 b5 91 2e ec 15 98
0080  ad b1 f7 52 5d 3a 2b 16 a9 44 d7 af 13 d1 0d 52
0090  fd cc 99 21
```

4) Identify if unencrypted communication is happening between client and server?

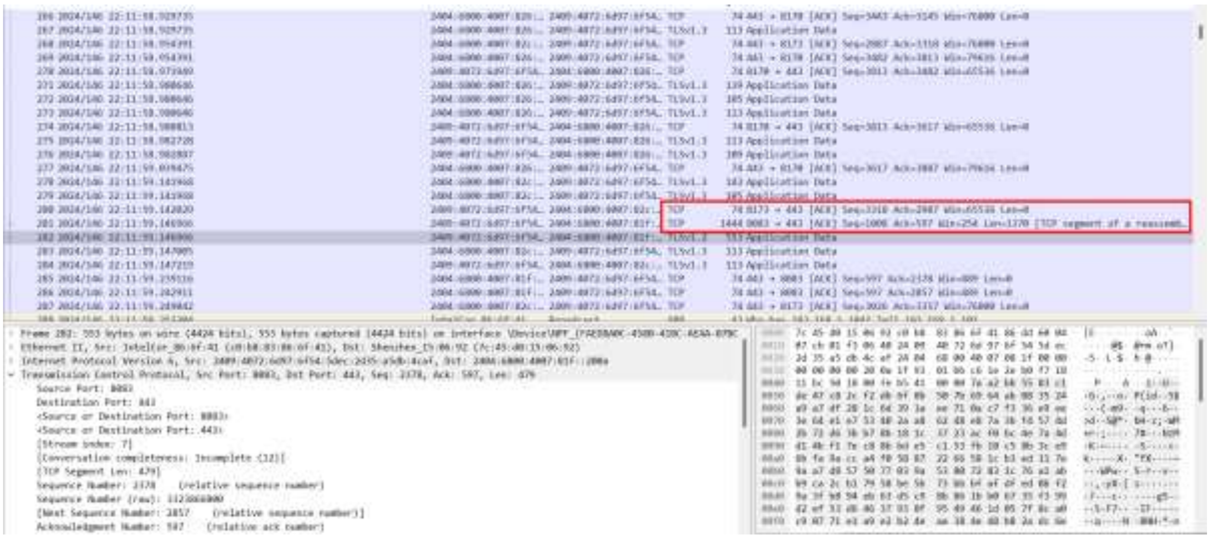
- In this case we can use either ECHIMIRAGE / wireshark. We have used Echomirage here.
- From the output we can see that when we login to DVTA , the data is sent as plaintext format to the database.



```
Outbound TCP data to 192.168.56.110:1433
        00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F   0123456789ABCDEF
0x0000  01 09 00 B2 00 00 01 00 16 00 00 00 12 00 00 00   ..*.............
0x0010  02 00 00 00 00 00 00 00 00 00 01 00 00 00 73 00   ..............s.
0x0020  65 00 6C 00 65 00 63 00 74 00 20 00 69 00 74 00   e.l.e.c.t. .i.t.
0x0030  65 00 6D 00 2C 00 20 00 70 00 72 00 69 00 63 00   e.m.,. .p.r.i.c.
0x0040  65 00 2C 00 20 00 64 00 61 00 74 00 65 00 2C 00   e.,. .d.a.t.e.,.
0x0050  74 00 69 00 6D 00 65 00 20 00 66 00 72 00 6F 00   t.i.m.e. .f.r.o.
0x0060  6D 00 20 00 65 00 78 00 70 00 65 00 6E 00 73 00   m. .e.x.p.e.n.s.
0x0070  65 00 73 00 20 00 77 00 68 00 65 00 72 00 65 00   e.s. .w.h.e.r.e.
0x0080  20 00 65 00 6D 00 61 00 69 00 6C 00 3D 00 27 00    .e.m.a.i.l.=.'.
0x0090  72 00 61 00 79 00 6D 00 6F 00 6E 00 64 00 40 00   r.a.y.m.o.n.d.@.
0x00A0  74 00 65 00 73 00 74 00 2E 00 63 00 6F 00 6D 00   t.e.s.t...c.o.m.
0x00B0  27 00                                             '.
```

5) Capture and analyse the communication using proxy tools (eg: Burpsuite, Echo mirage).

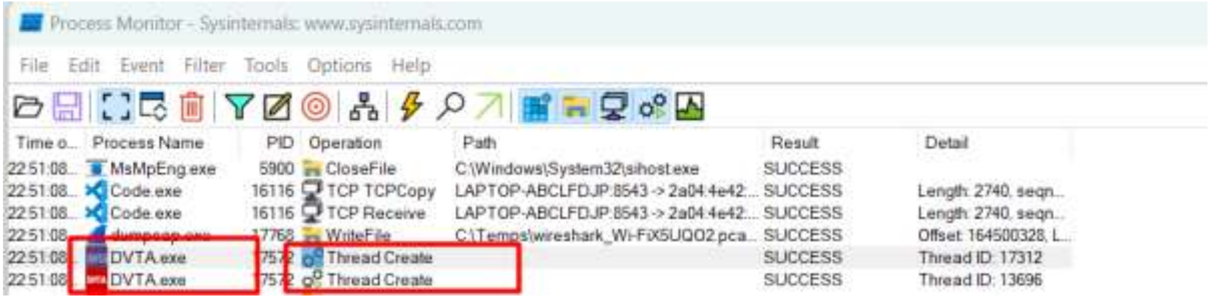
- From the below screenshot, we can understand that using wireshark we're able to capture & analyse the requests that are being sent to the database and to the server.



```
> Frame 282: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface \Device\NPF_{[illegible]}
> Ethernet II, Src: IntelCor_[illegible], Dst: Shenzhen_[illegible]
> Internet Protocol Version 6, Src: 2409:4072:[illegible], Dst: 2404:6800:4007:81f::200a
v Transmission Control Protocol, Src Port: 8083, Dst Port: 443, Seq: 2378, Ack: 597, Len: 479
    Source Port: 8083
    Destination Port: 443
    <Source or Destination Port: 8083>
    <Source or Destination Port: 443>
    [Stream index: 7]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 479]
    Sequence Number: 2378    (relative sequence number)
    Sequence Number (raw): [illegible]
    [Next Sequence Number: 2857    (relative sequence number)]
    Acknowledgment Number: 597    (relative ack number)
```

6) Analyse the application workflow and observe which all files/folders are being used by the application using Process Monitor

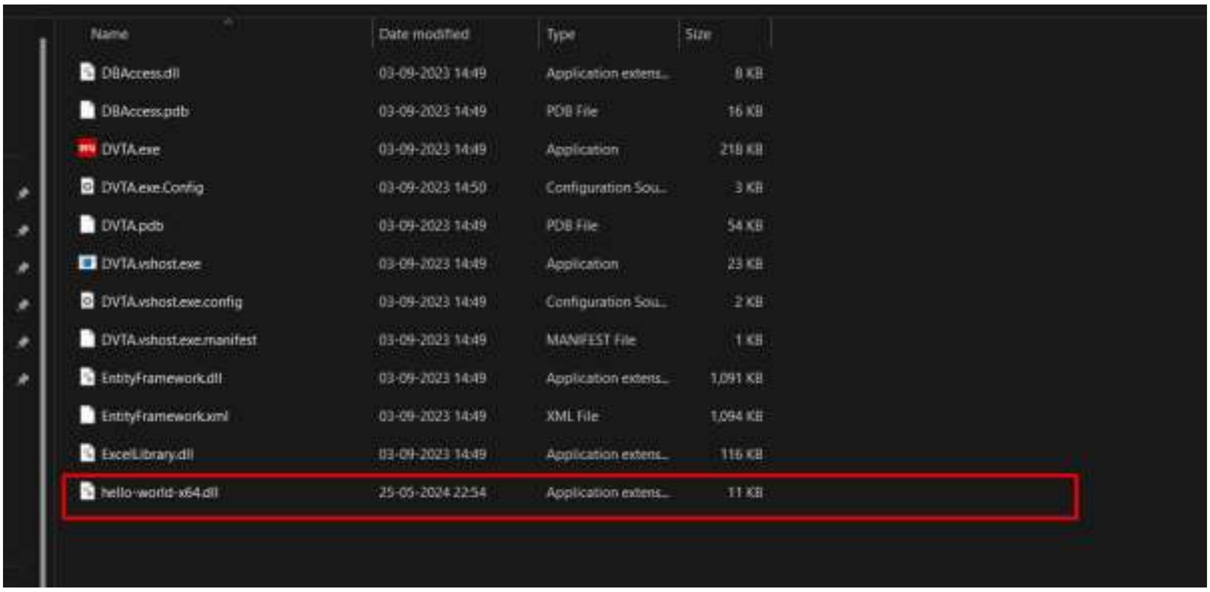
- With the help of a tool called Process-Monitor can see that there are several files & folders being retrieved when running the DVTA.exe.



Time o...	Process Name	PID	Operation	Path	Result	Detail
22:51:08...	MsMpEng.exe	5900	CloseFile	C:\Windows\System32\sihost.exe	SUCCESS	
22:51:08...	Code.exe	16116	TCP TCPCopy	LAPTOP-ABCLFDJP:8543 -> 2a04:4e42:...	SUCCESS	Length: 2740, seqn...
22:51:08...	Code.exe	16116	TCP Receive	LAPTOP-ABCLFDJP:8543 -> 2a04:4e42:...	SUCCESS	Length: 2740, seqn...
22:51:08...	dumpcap.exe	17768	WriteFile	C:\Temps\wireshark_Wi-FiX5UQO2.pca...	SUCCESS	Offset: 164500328, L...
22:51:08...	DVTA.exe	7572	Thread Create		SUCCESS	Thread ID: 17312
22:51:08...	DVTA.exe	7572	Thread Create		SUCCESS	Thread ID: 13696

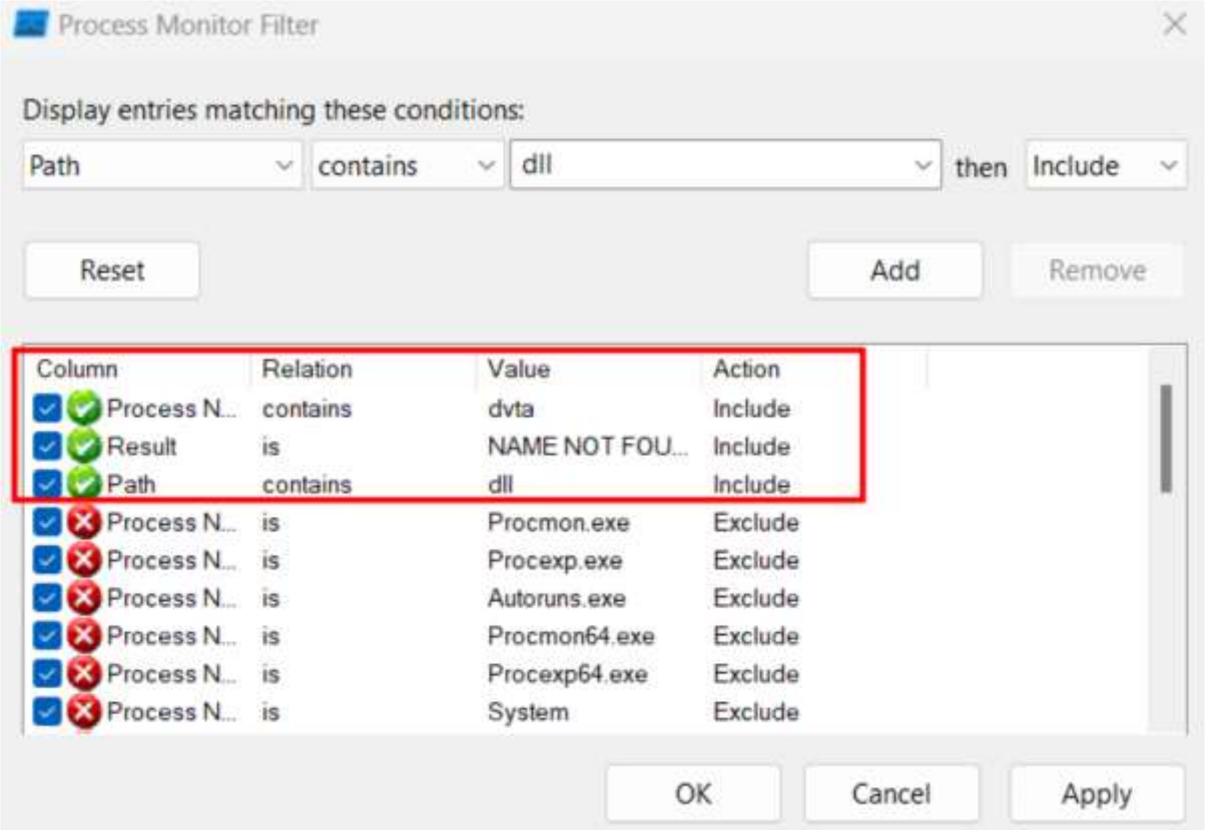
7) Exploit DLL Hijacking vulnerability (You can use a simple legitimate "Hello World" printing dll.

- In order to hijack a DLL, we need to find which DLL's that are being loaded when DVTA.exe runs is not found.
- For this we need to open Procmon & set the following 3 filters .



Name	Date modified	Type	Size
DBAccess.dll	03-09-2023 14:49	Application extens...	8 KB
DBAccess.pdb	03-09-2023 14:49	PDB File	16 KB
DVTA.exe	03-09-2023 14:49	Application	218 KB
DVTA.exe.Config	03-09-2023 14:50	Configuration Sou...	3 KB
DVTA.pdb	03-09-2023 14:49	PDB File	54 KB
DVTA.vshost.exe	03-09-2023 14:49	Application	23 KB
DVTA.vshost.exe.config	03-09-2023 14:49	Configuration Sou...	2 KB
DVTA.vshost.exe.manifest	03-09-2023 14:49	MANIFEST File	1 KB
EntityFramework.dll	03-09-2023 14:49	Application extens...	1,091 KB
EntityFramework.xml	03-09-2023 14:49	XML File	1,094 KB
ExcelLibrary.dll	03-09-2023 14:49	Application extens...	116 KB
hello-world-x64.dll	25-05-2024 22:54	Application extens...	11 KB

- We will Start Process Monitor Filter



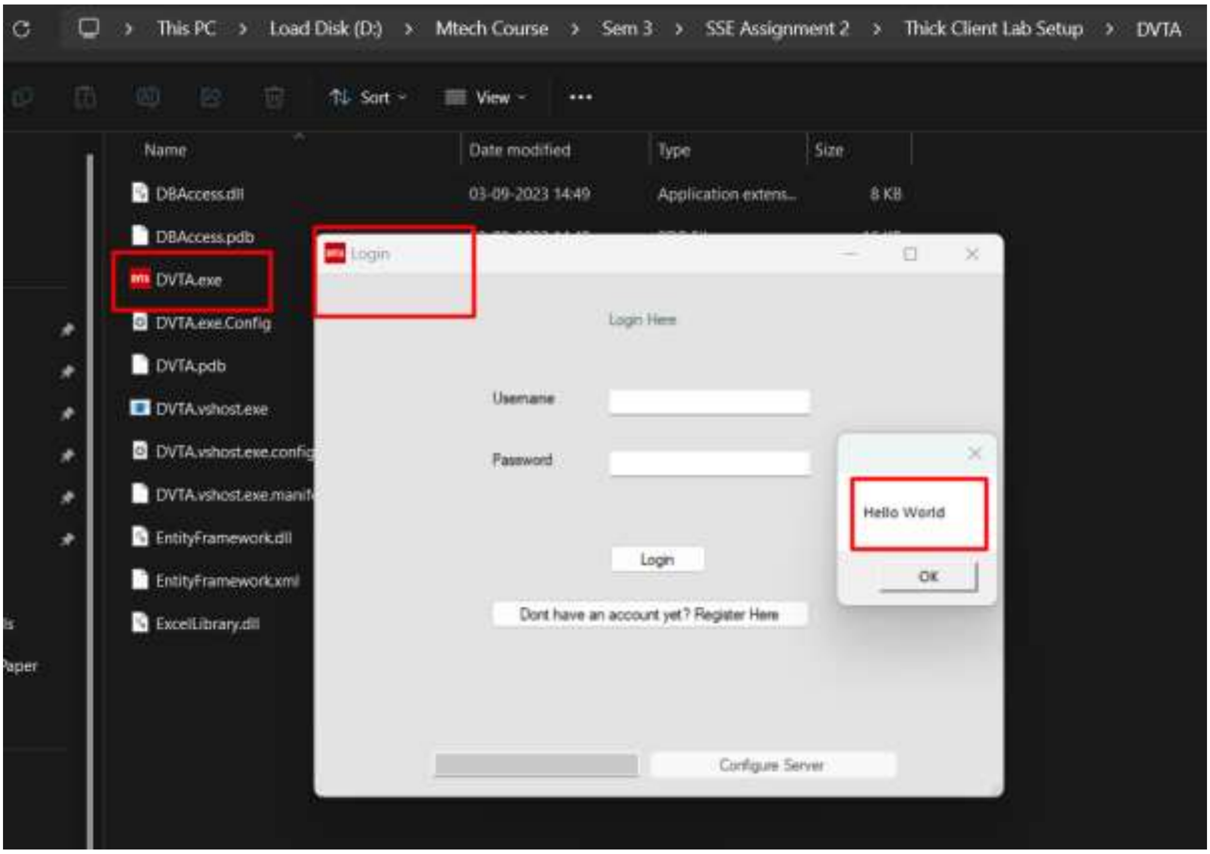
Process Monitor Filter

Display entries matching these conditions:

Path | contains | dll | then | Include

Column	Relation	Value	Action
☑ ✓ Process N...	contains	dvta	Include
☑ ✓ Result	is	NAME NOT FOU...	Include
☑ ✓ Path	contains	dll	Include
☑ ✕ Process N...	is	Procmon.exe	Exclude
☑ ✕ Process N...	is	Procexp.exe	Exclude
☑ ✕ Process N...	is	Autoruns.exe	Exclude
☑ ✕ Process N...	is	Procmon64.exe	Exclude
☑ ✕ Process N...	is	Procexp64.exe	Exclude
☑ ✕ Process N...	is	System	Exclude

- When click DVTA.exe automatically Hello world pop up will appear with opening of DVTA Login Page



This PC > Load Disk (D:) > Mtech Course > Sem 3 > SSE Assignment 2 > Thick Client Lab Setup > DVTA

Name	Date modified	Type	Size
DBAccess.dll	03-09-2023 14:49	Application extens...	8 KB
DBAccess.pdb			
DVTA.exe			
DVTA.exe.Config			
DVTA.pdb			
DVTA.vshost.exe			
DVTA.vshost.exe.config			
DVTA.vshost.exe.manif			
EntityFramework.dll			
EntityFramework.xml			
ExcelLibrary.dll			

Login

Login Here

Username

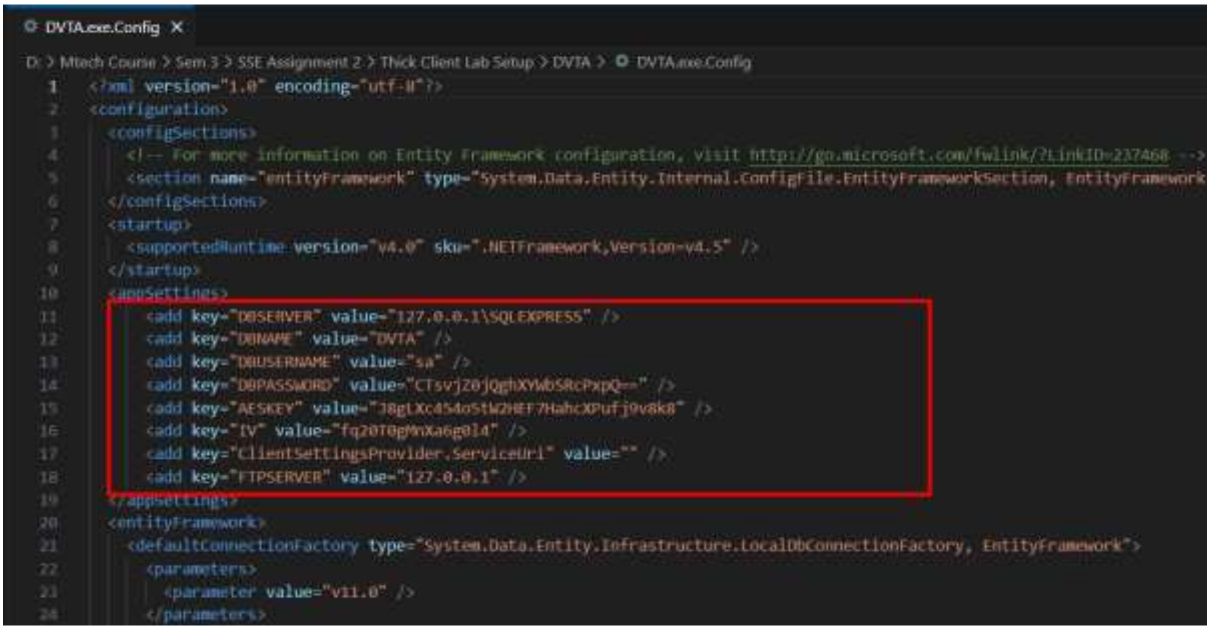
Password

Hello World

- As we can see now when the DVTA.exe runs, it loads our calc.dll along with the application. Thus we have hijacked the DLL.

8) Check for sensitive information in the configuration files of the thick client application?

- In the folder of DVTA, we have few files . One of the files is App.config. It contains the following sensitive information.
- We have to open Visual Studio and analyse DVTA.exe.config.

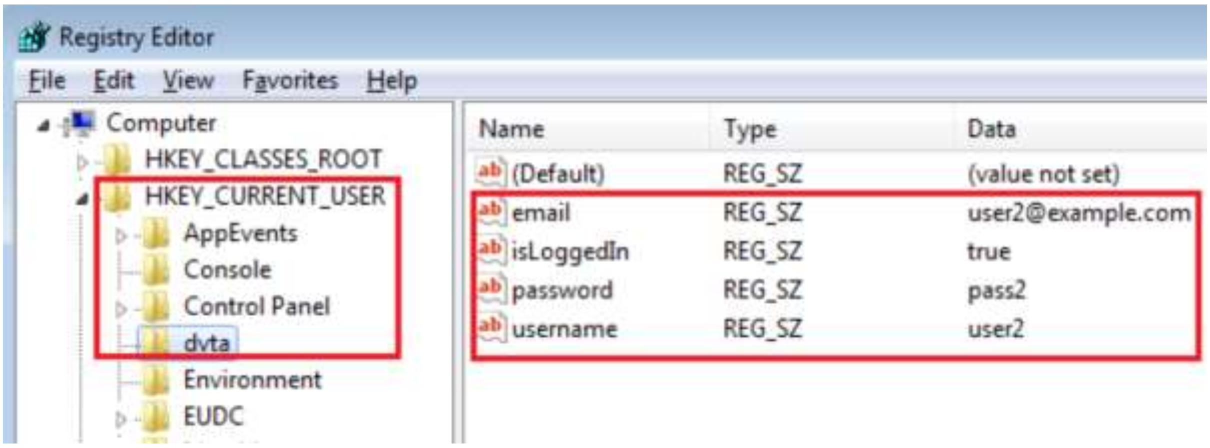


DVTA.exe.Config ×
D: > Mtech Course > Sem 3 > SSE Assignment 2 > Thick Client Lab Setup > DVTA > DVTA.exe.Config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <appSettings>
      <add key="DBSERVER" value="127.0.0.1\SQLEXPRESS" />
      <add key="DBNAME" value="DVTA" />
      <add key="DBUSERNAME" value="sa" />
      <add key="DBPASSWORD" value="CTsvjZ0jQghXYWbSRcPxpQ==" />
      <add key="AESKEY" value="J8gLXc454o5tW2HEF7HahcXPufj9v8k8" />
      <add key="IV" value="fq20T0gMnXa6g0l4" />
      <add key="ClientSettingsProvider.ServiceUri" value="" />
      <add key="FTPSERVER" value="127.0.0.1" />
  </appSettings>
  <entityFramework>
    <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
      <parameters>
        <parameter value="v11.0" />
      </parameters>
```

9) Identify sensitive information found in memory?

- From the source code which we got from DNSpy, we got to know that it stores the username & password in HKCU/dvta registry file.
- We can visit the registry to find the sensitive information which is stored in the memory.
- We have to open registry editor to analyse dvta username and password.



Name	Type	Data
(Default)	REG_SZ	(value not set)
email	REG_SZ	user2@example.com
isLoggedIn	REG_SZ	true
password	REG_SZ	pass2
username	REG_SZ	user2