K P Uday Krishna
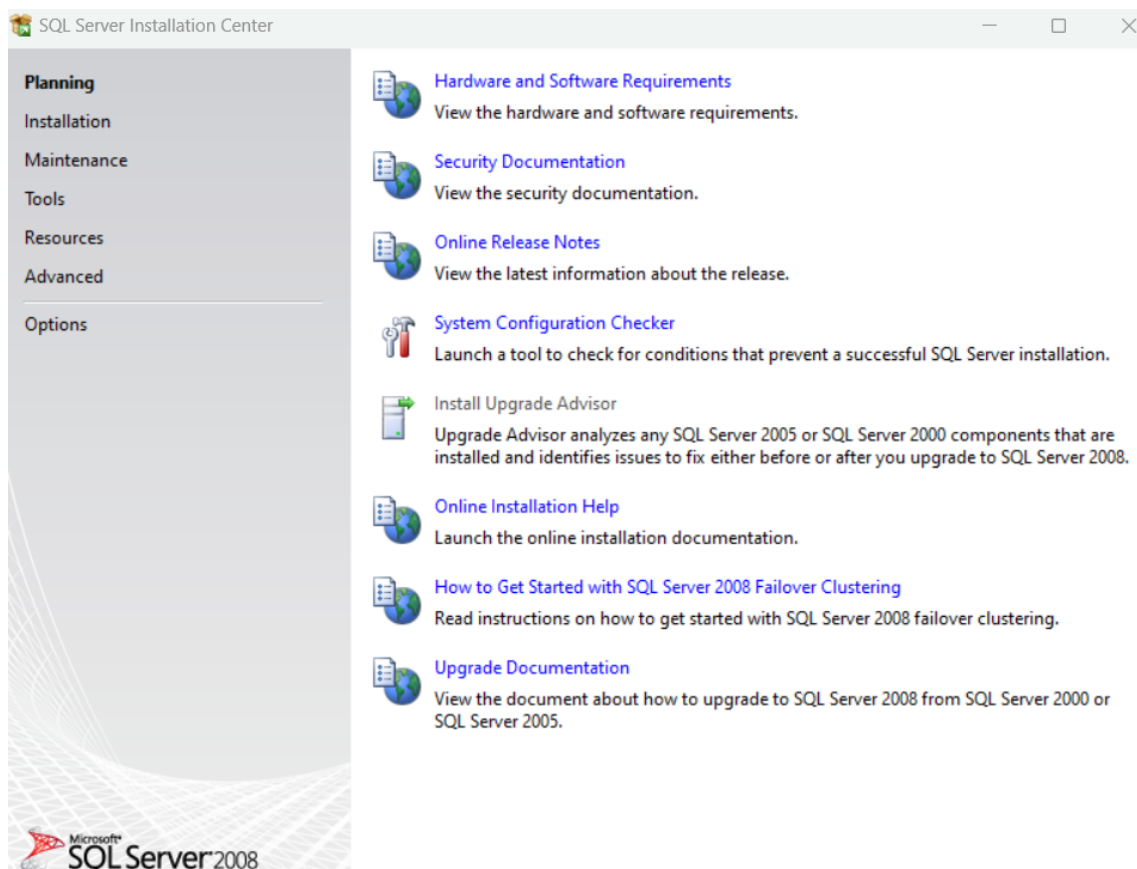
CB.SC.P2CYS23012
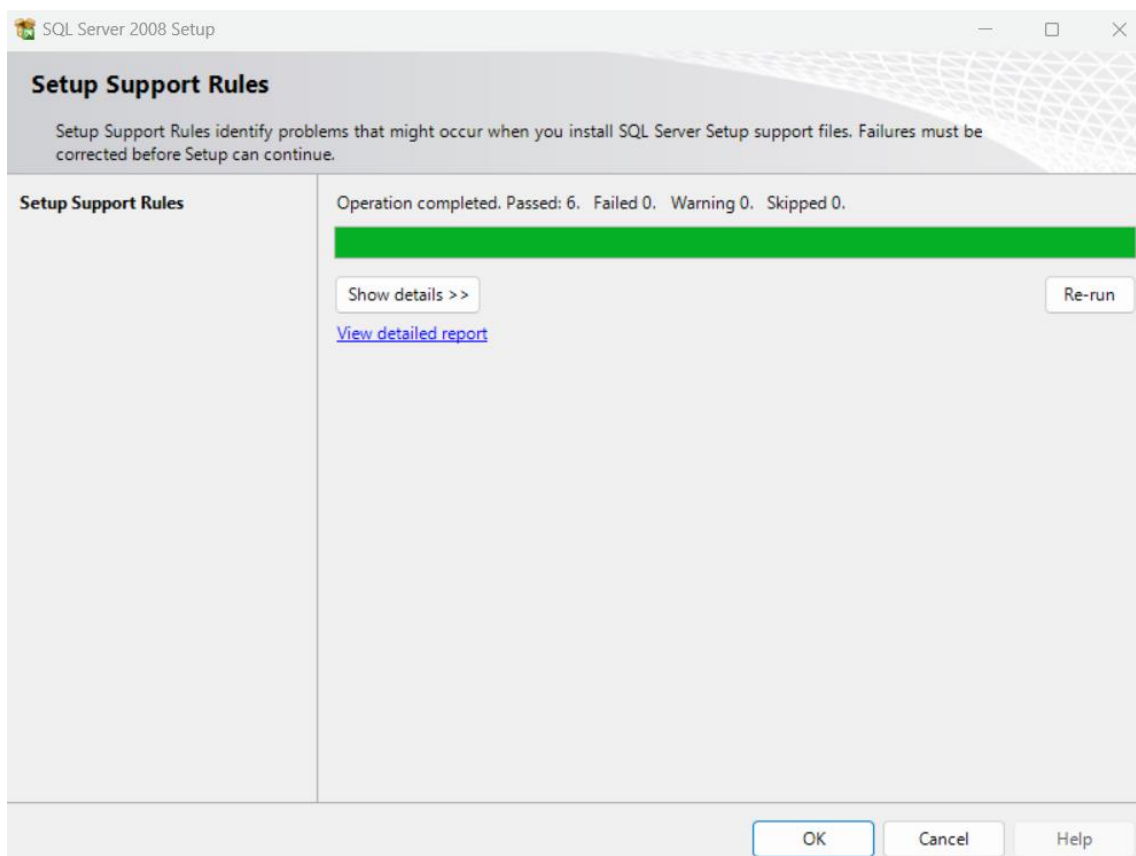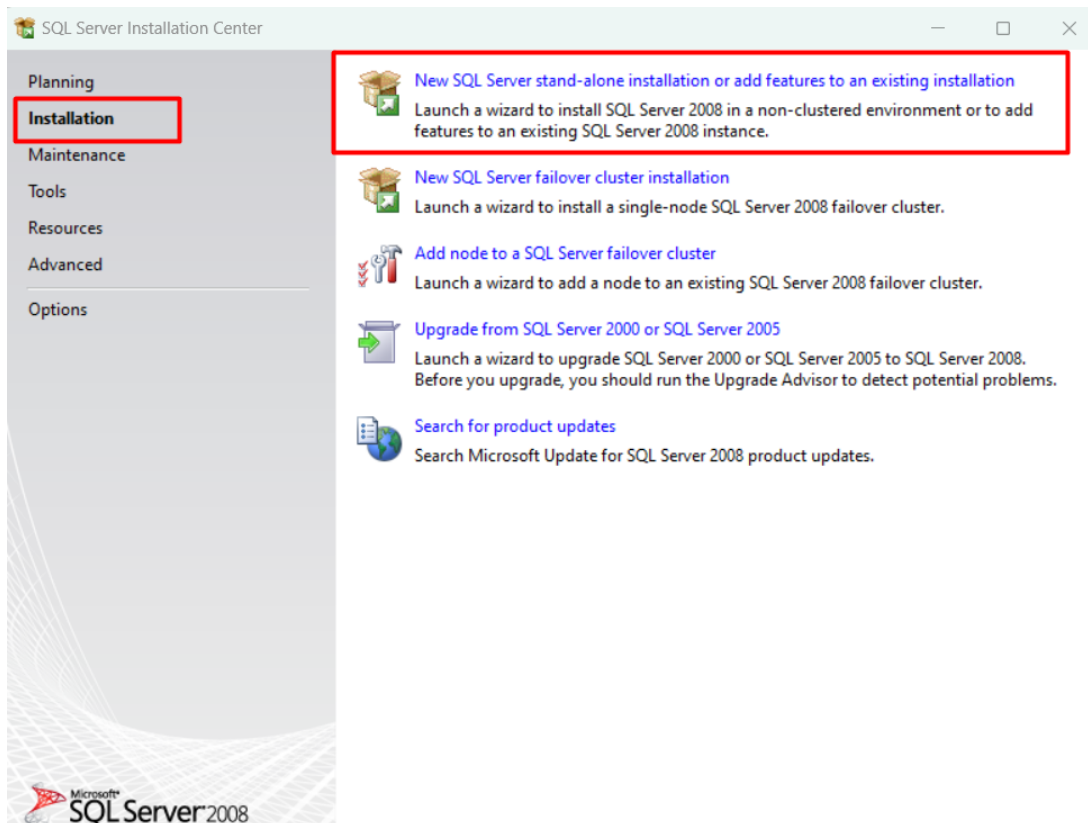
SSE Assignment 2

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

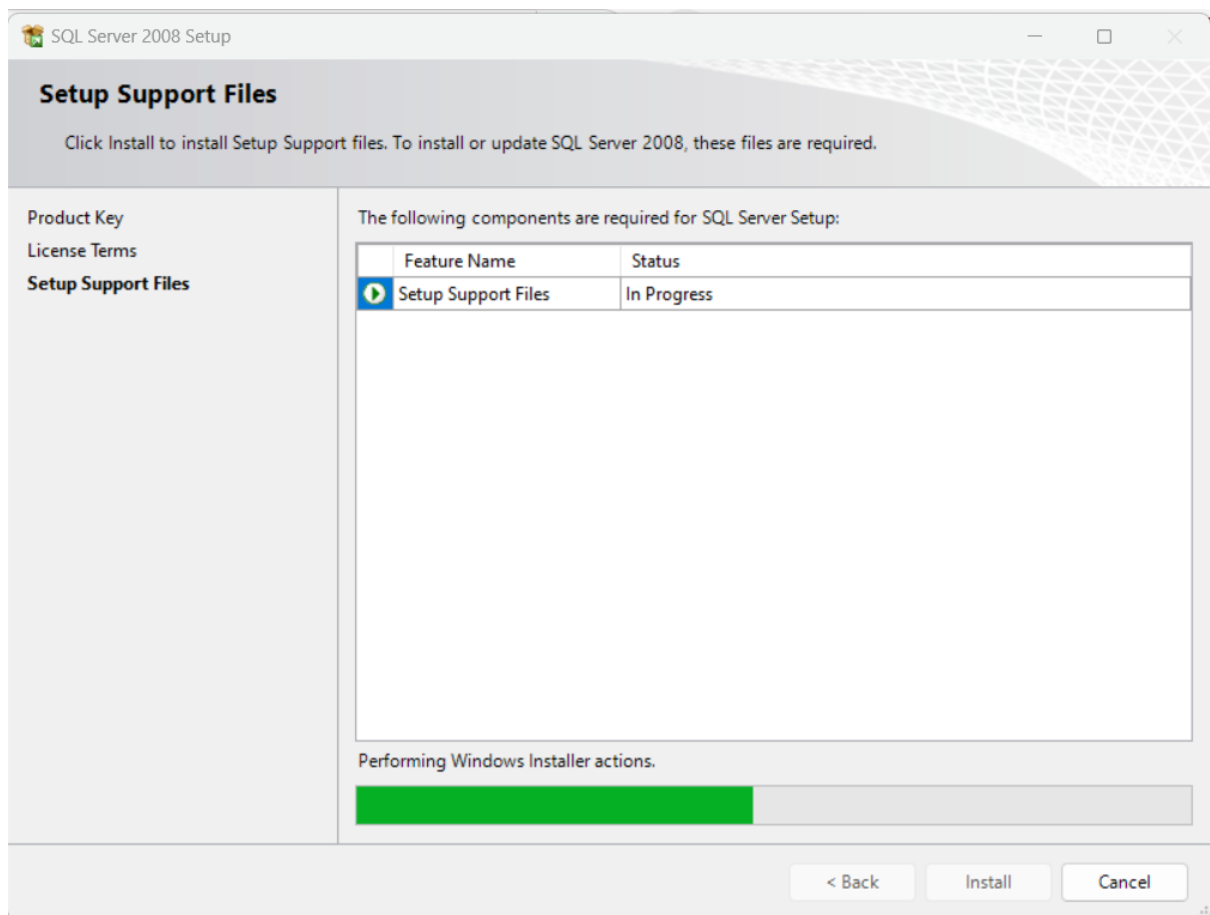## Use CFF Framework to analyse custom DVTA.exe created above.

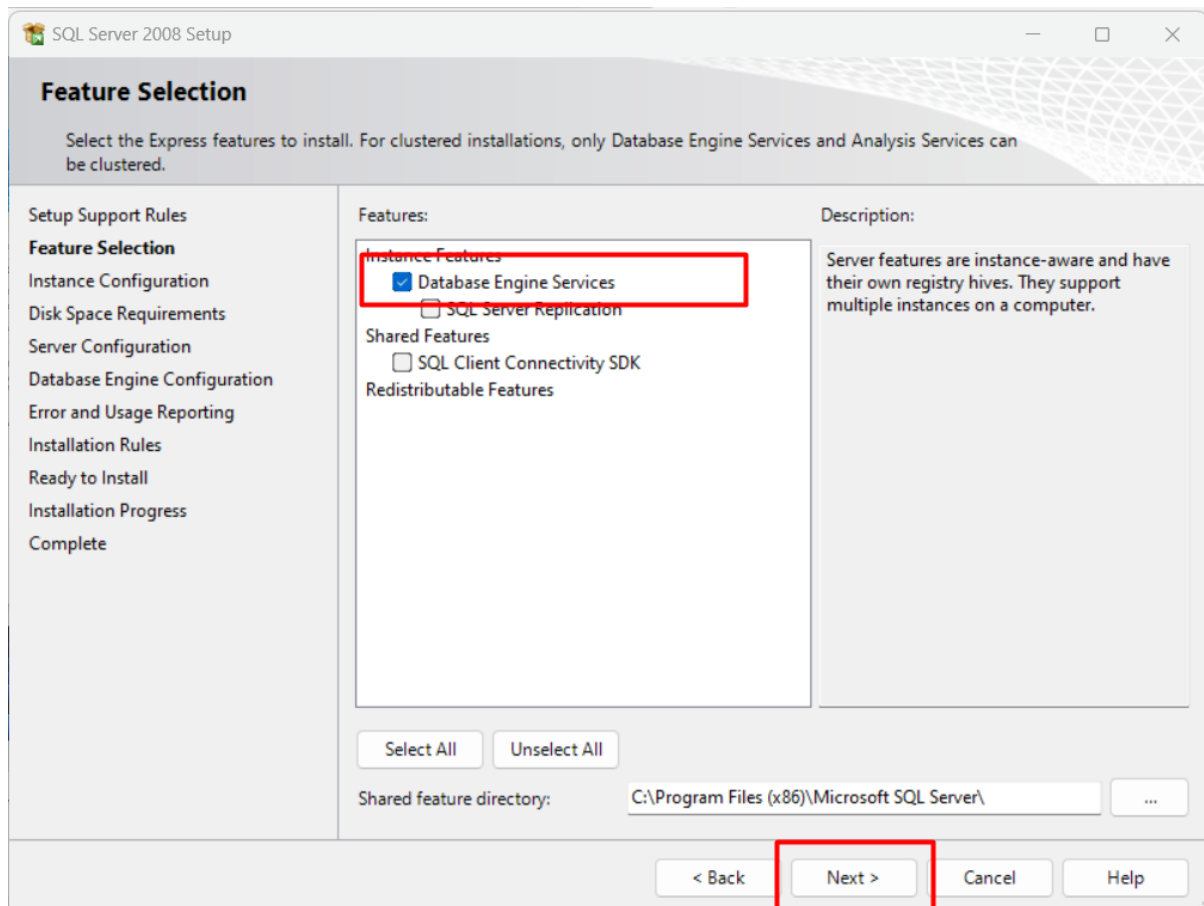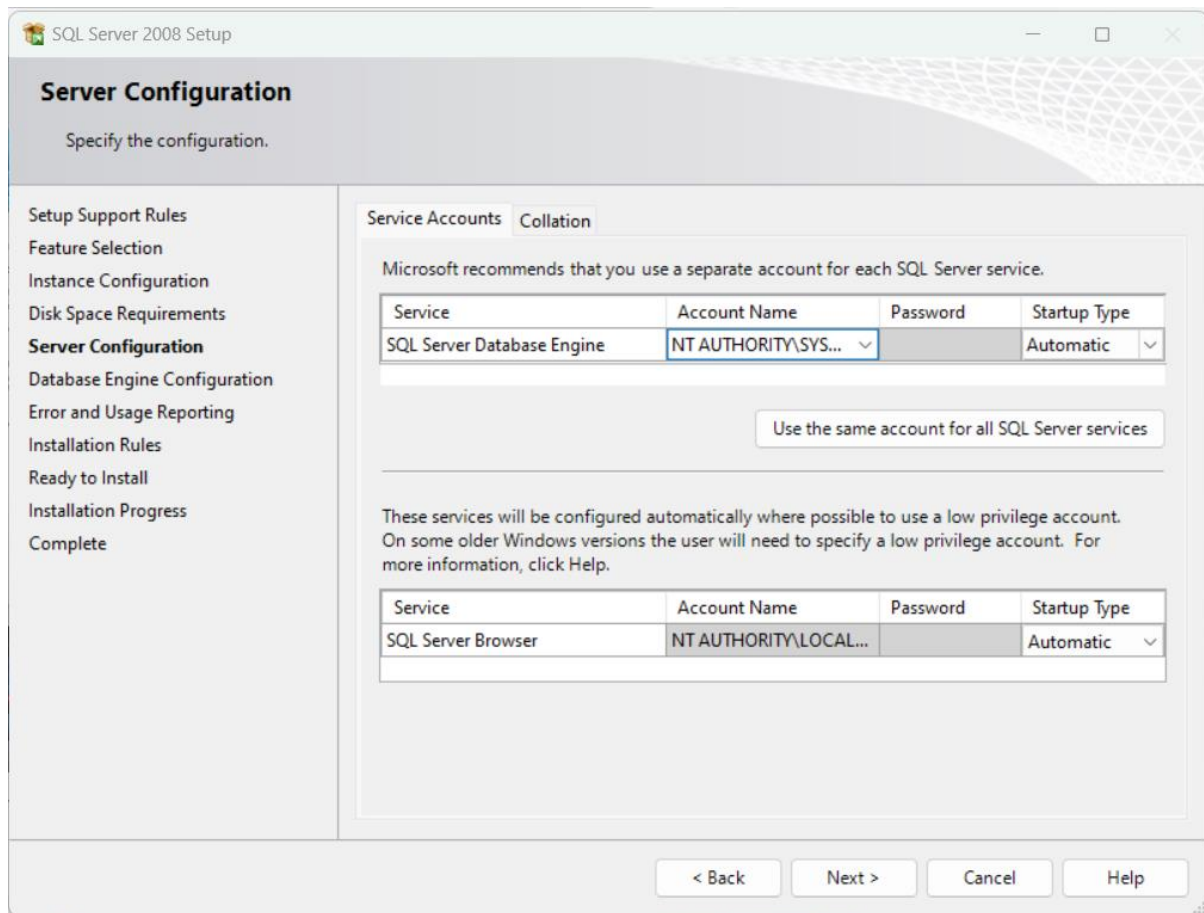To Start with the DVTA, first we need to setup SQL Server 2008

We have to setup support files

To Add Database Engine

Now we have to configure server

Add a password as a configuration of Server

Password Should be – P@ssw0rd

- We need to add users SQL Server Administrator

SQL Server 2008 Setup

Database Engine Configuration

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

Setup Support Rules
Feature Selection
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error and Usage Reporting
Installation Rules
Ready to Install
Installation Progress
Complete

Account Provisioning | Data Directories | User Instances

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

LAPTOP-ABCLFDJP\Jay Shah 17 (Jay Shah 17)

SQL Server administrators have unrestricted access to the Database Engine.

Add Current User   Add...   Remove

< Back   Next >   Cancel   Help

SQL Server 2008 Setup

Installation Progress

Setup Support Rules
Feature Selection
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error and Usage Reporting
Installation Rules
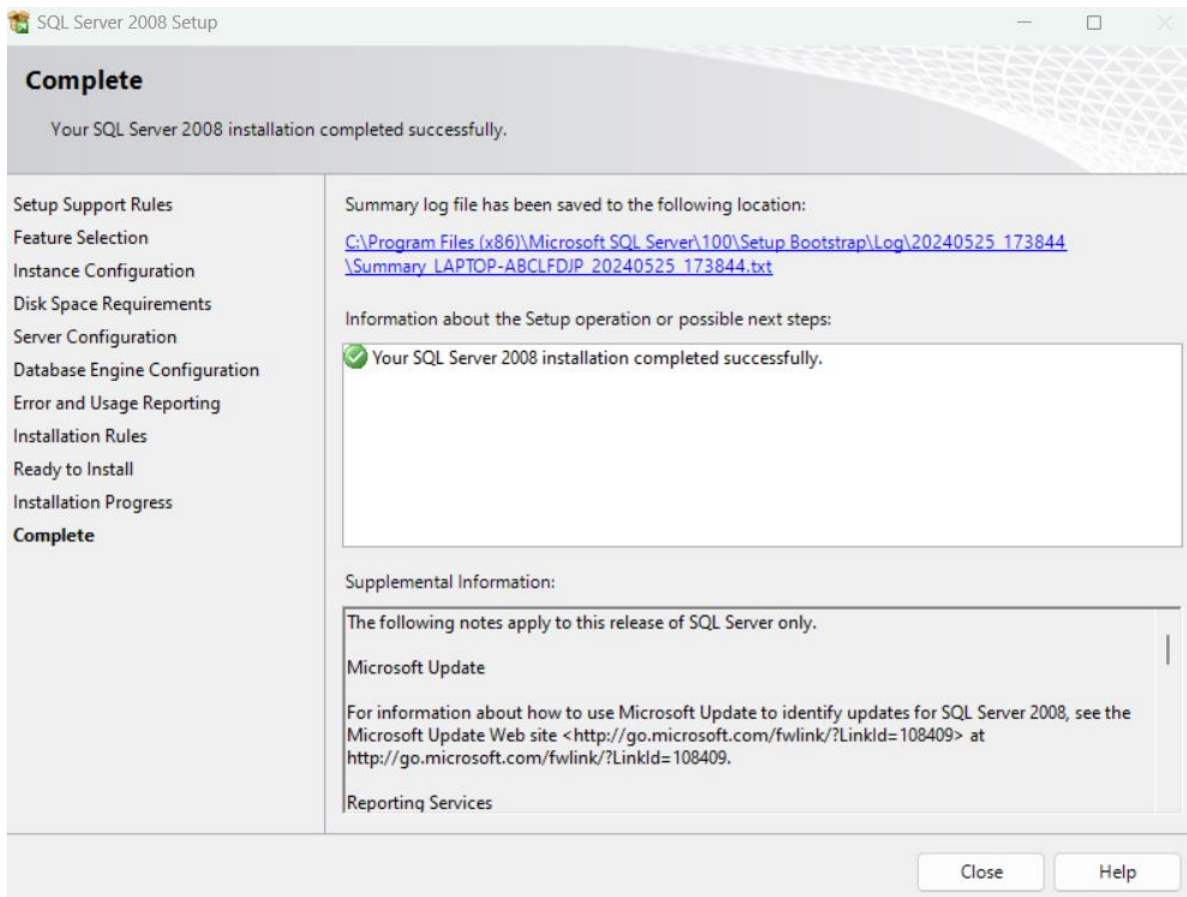Ready to Install
Installation Progress
Complete

Running post-Windows Installer configuration timing actions.
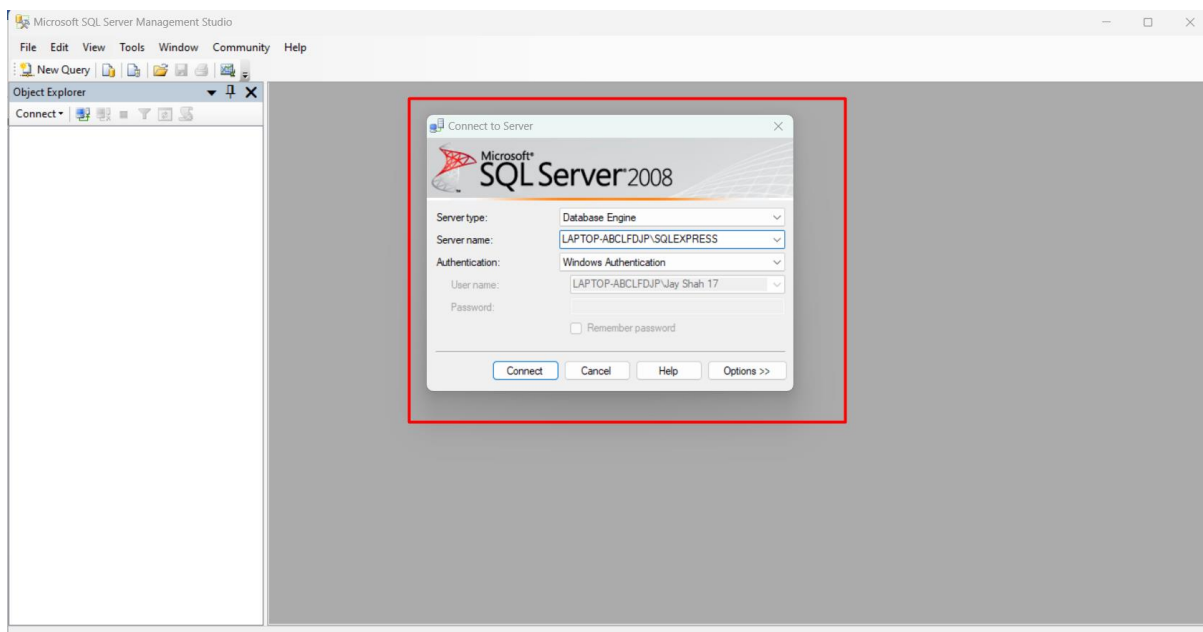
SqlBrowserConfigEngAction_install_ConfigNonRC_Cpu32

Next >   Cancel   Help
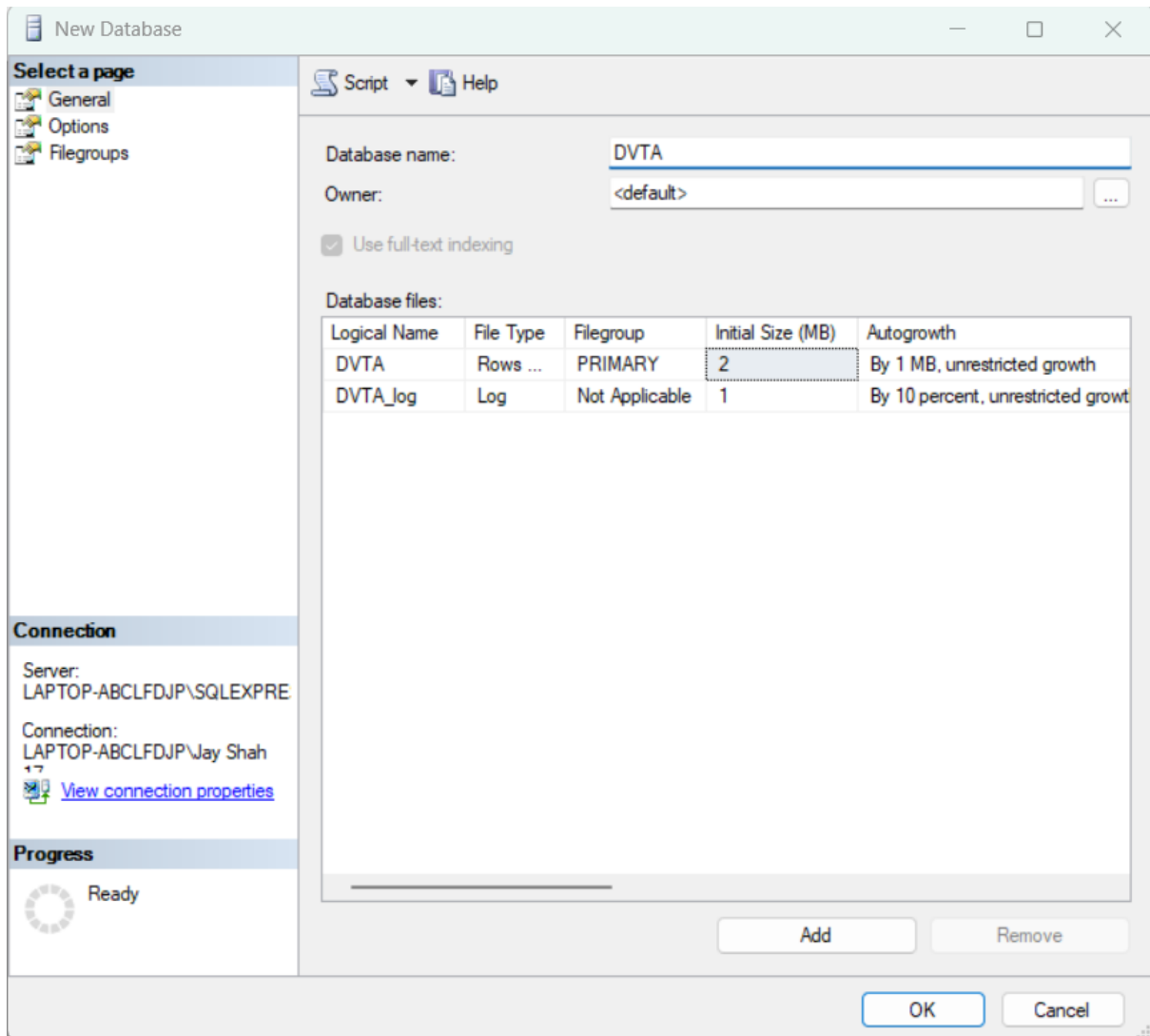
- We need to start SQL Server 2008

Create New Database

- Restart SQL Server

- Start a Filezila Server in your computer
- Going to Admin Panel
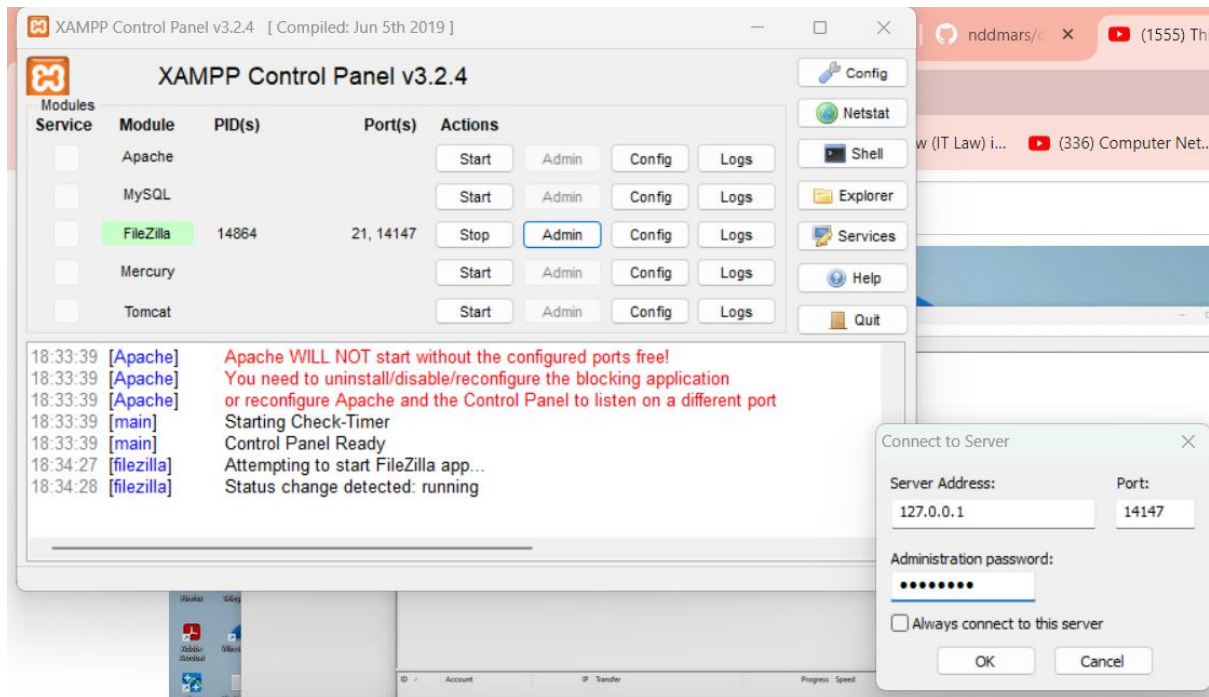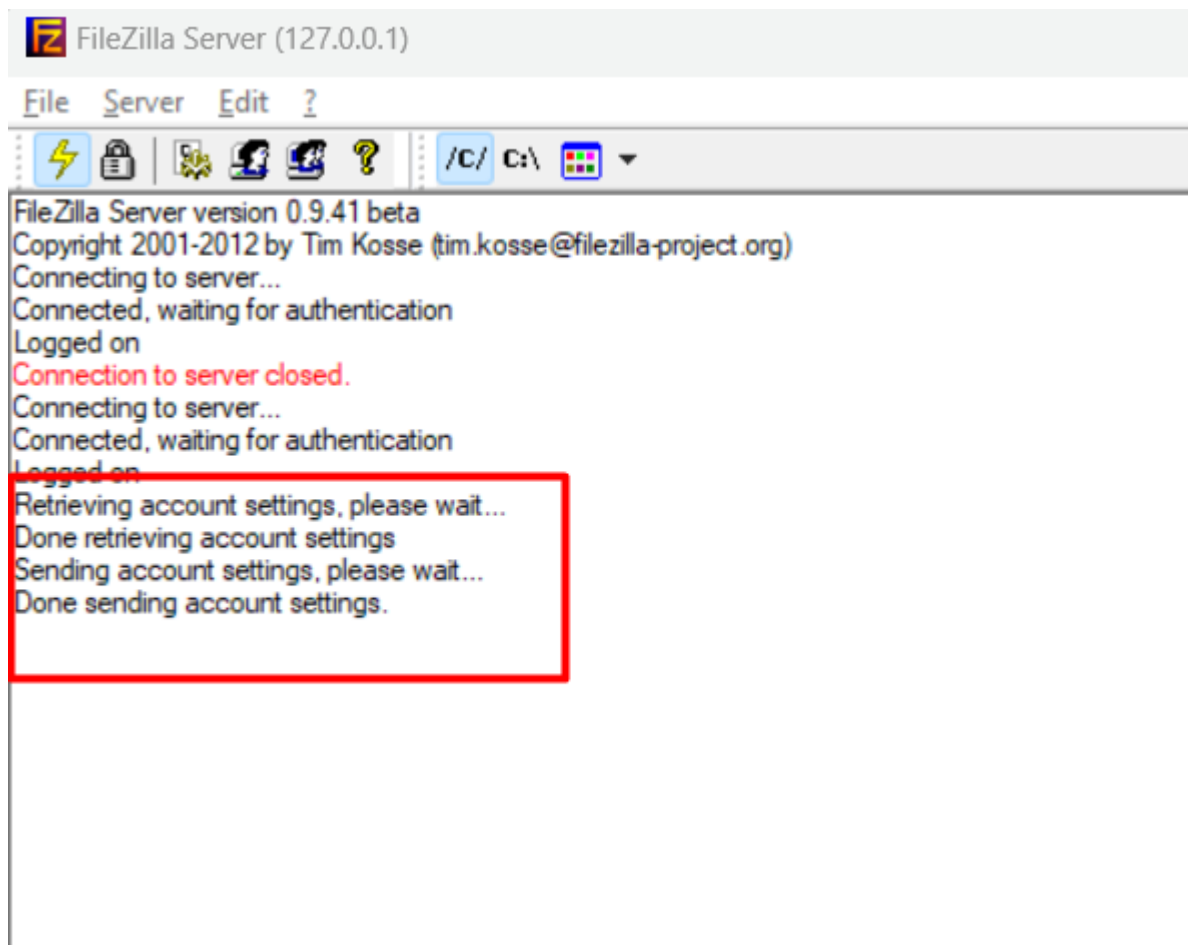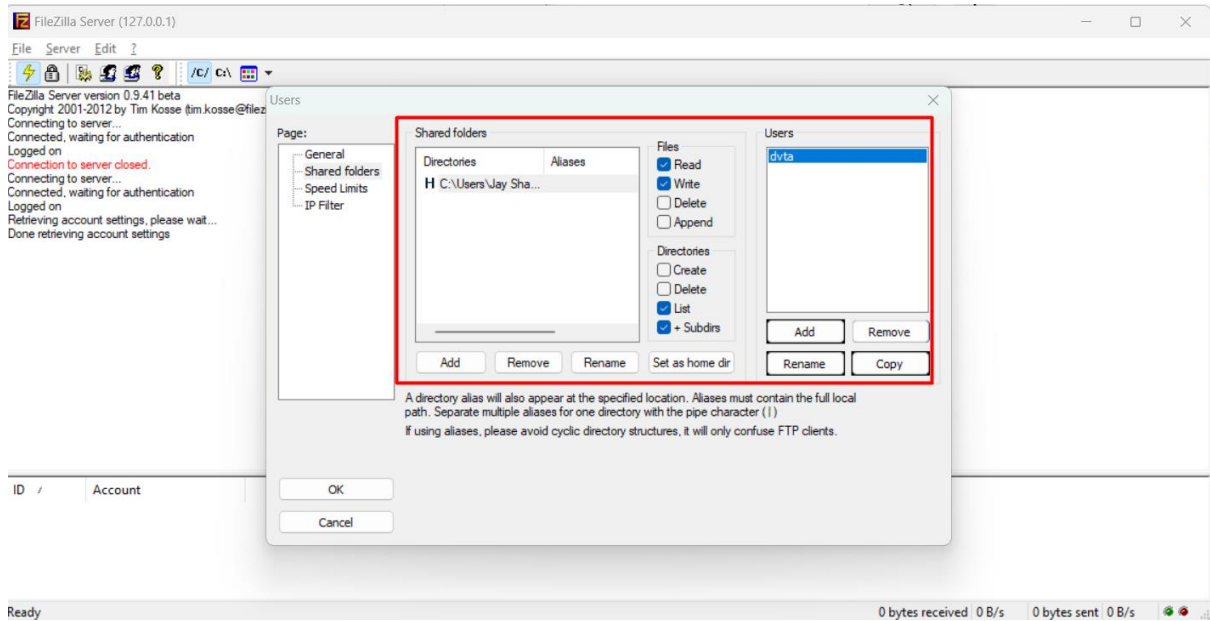
1) Identify the Application architecture, languages and frameworks used?

- 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

2. Decompile and try to retrieve the source code of the application? Also, check if any hardcoded sensitive information is found?
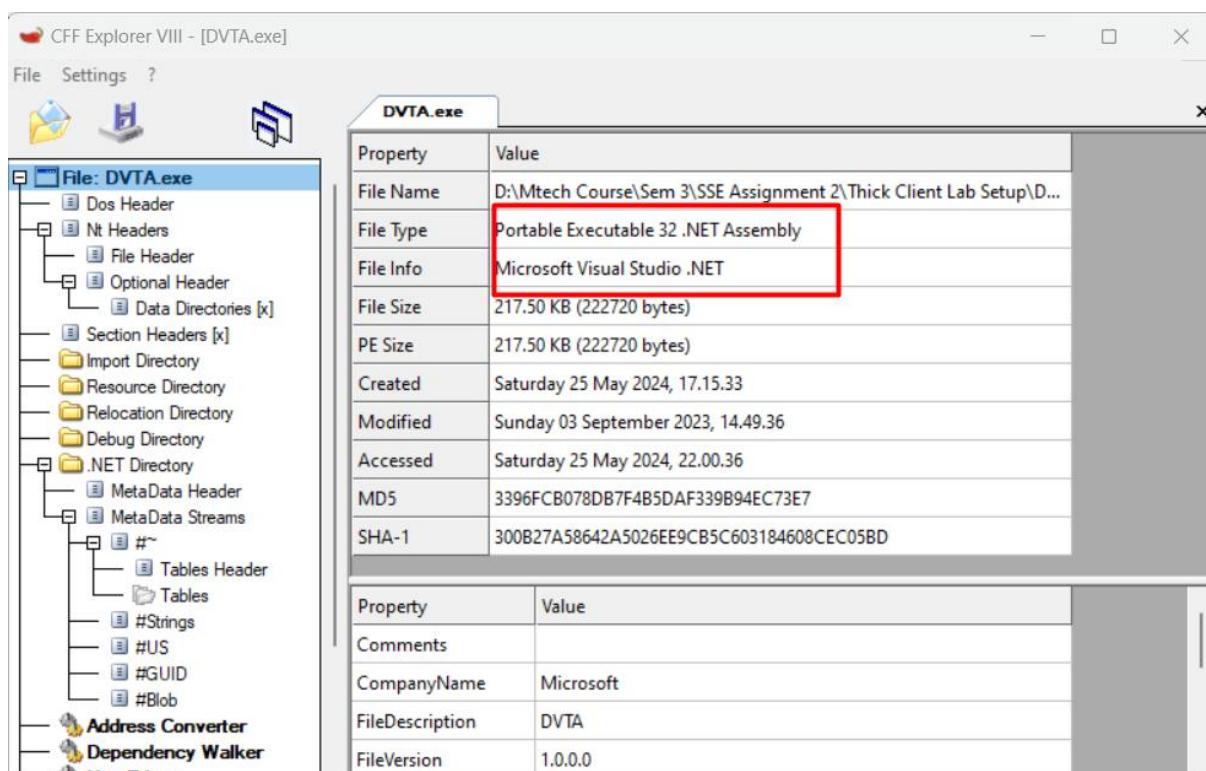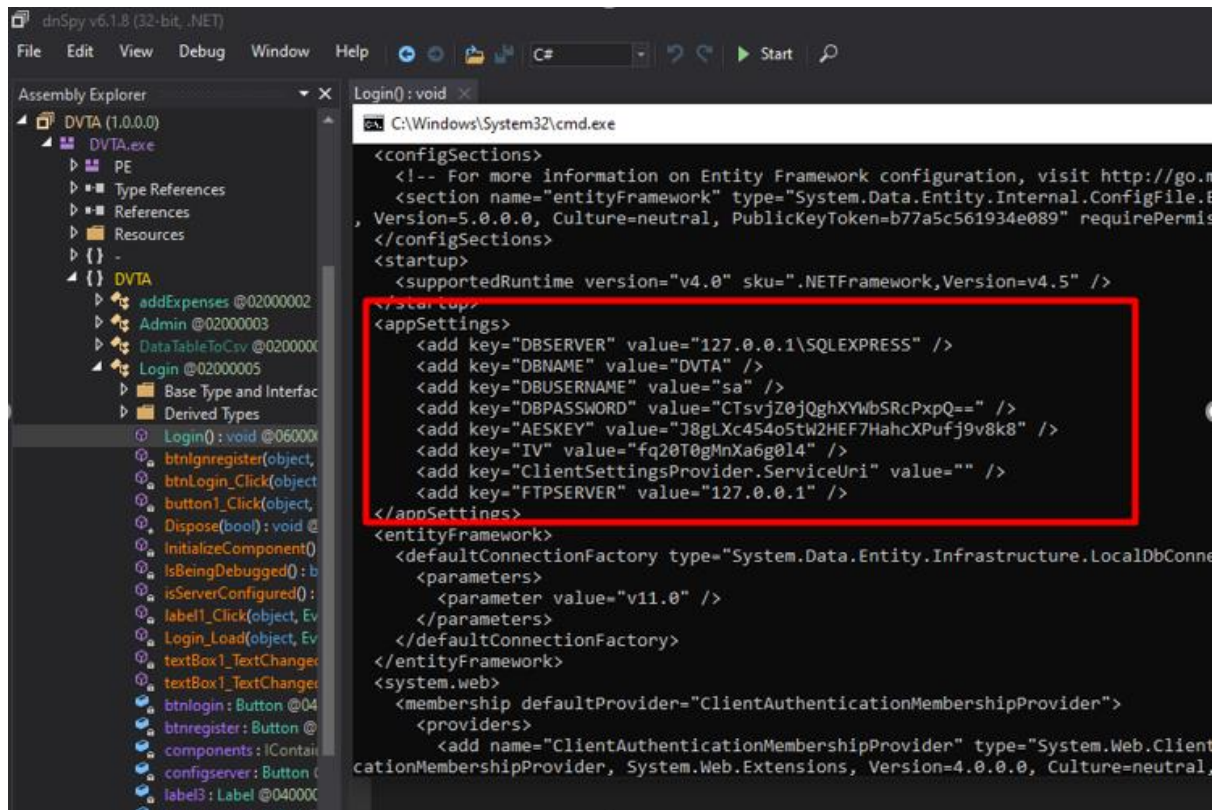
- By decompiling the application using DNSpy or MS Visual studio tools, we can see the source code of the application.

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.

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.

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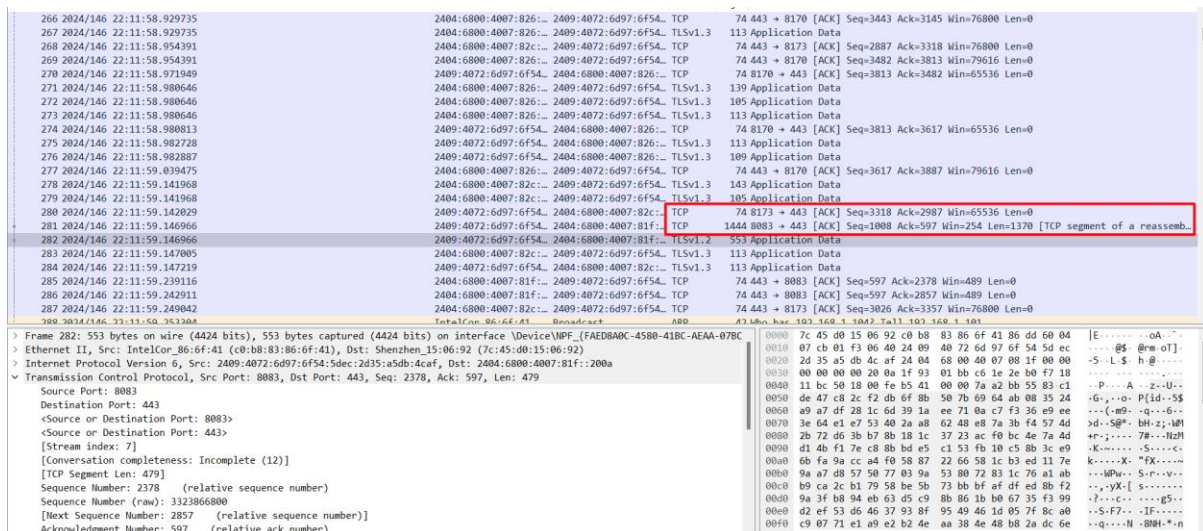
6) Analyse the application workflow and observe which all files/folders are being used by the application using Process Monitor

- With the help of a tool called Process-Monitor can see that there are several files & folders being retrieved when running the DVTA.exe.
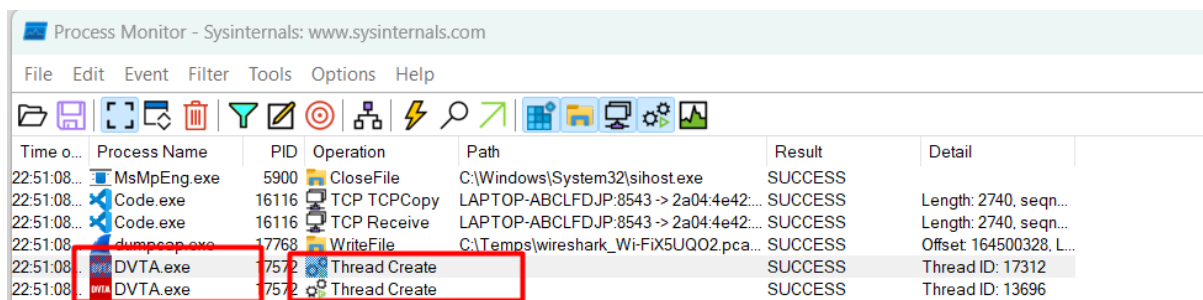
7) Exploit DLL Hijacking vulnerability (You can use a simple legitimate "Hello World" printing dll.

- 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 .

- We will Start Process Monitor Filter

- When click DVTA.exe automatically Hello world pop up will appear with opening of DVTA Login Page
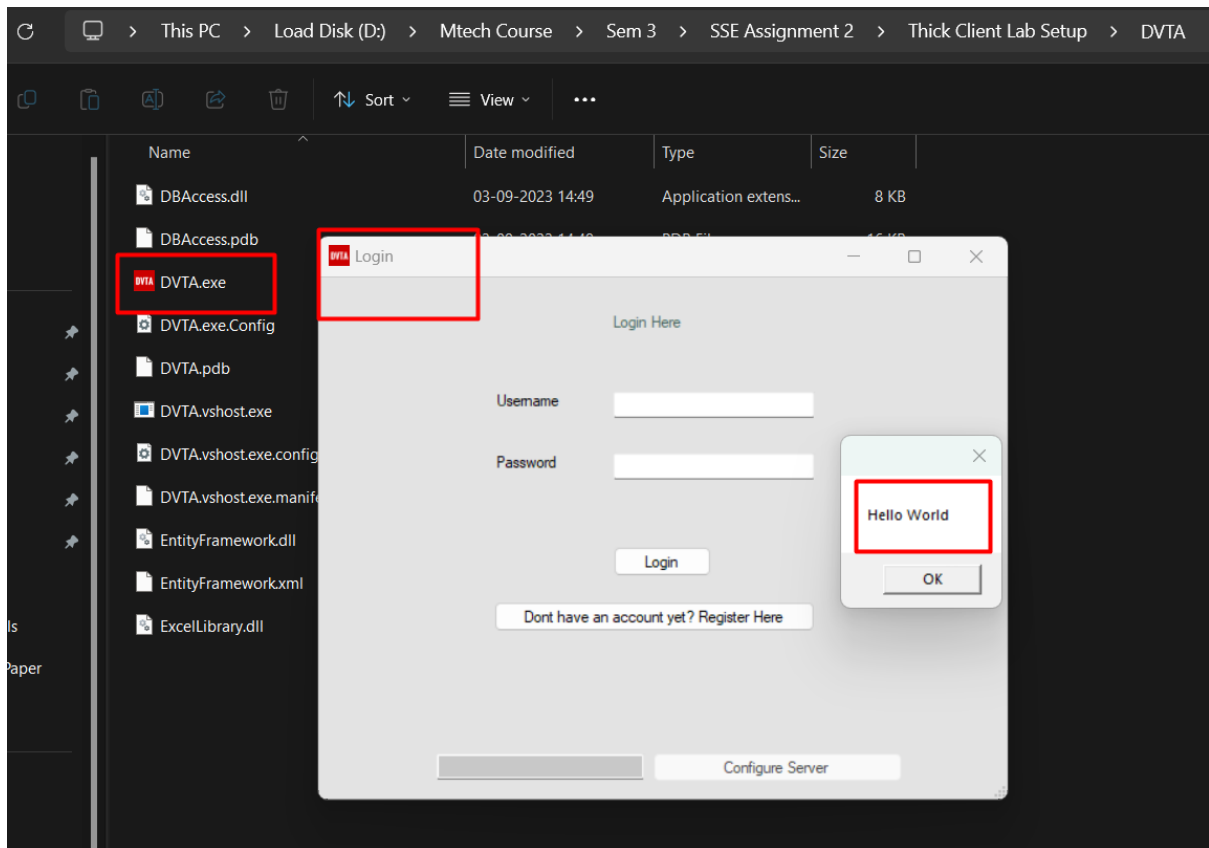
- As we can see now when the DVTA.exe runs, it loads our calc.dll along with the application. Thus we have hijacked the DLL.

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
   1   <?xml version="1.0" encoding="utf-8"?>
   2   <configuration>
   3     <configSections>
   4       <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->
   5       <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework
   6     </configSections>
   7     <startup>
   8       <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
   9     </startup>
  10     <appSettings>
  11       <add key="DBSERVER" value="127.0.0.1\SQLEXPRESS" />
  12       <add key="DBNAME" value="DVTA" />
  13       <add key="DBUSERNAME" value="sa" />
  14       <add key="DBPASSWORD" value="CTsvjZ0jQghXYWbSRcPxpQ==" />
  15       <add key="AESKEY" value="J8gLXc454o5tW2HEF7HahcXPufj9v8k8" />
  16       <add key="IV" value="fq20T0gMnXa6g0l4" />
  17       <add key="ClientSettingsProvider.ServiceUri" value="" />
  18       <add key="FTPSERVER" value="127.0.0.1" />
  19     </appSettings>
  20     <entityFramework>
  21       <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
  22         <parameters>
  23           <parameter value="v11.0" />
  24         </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.