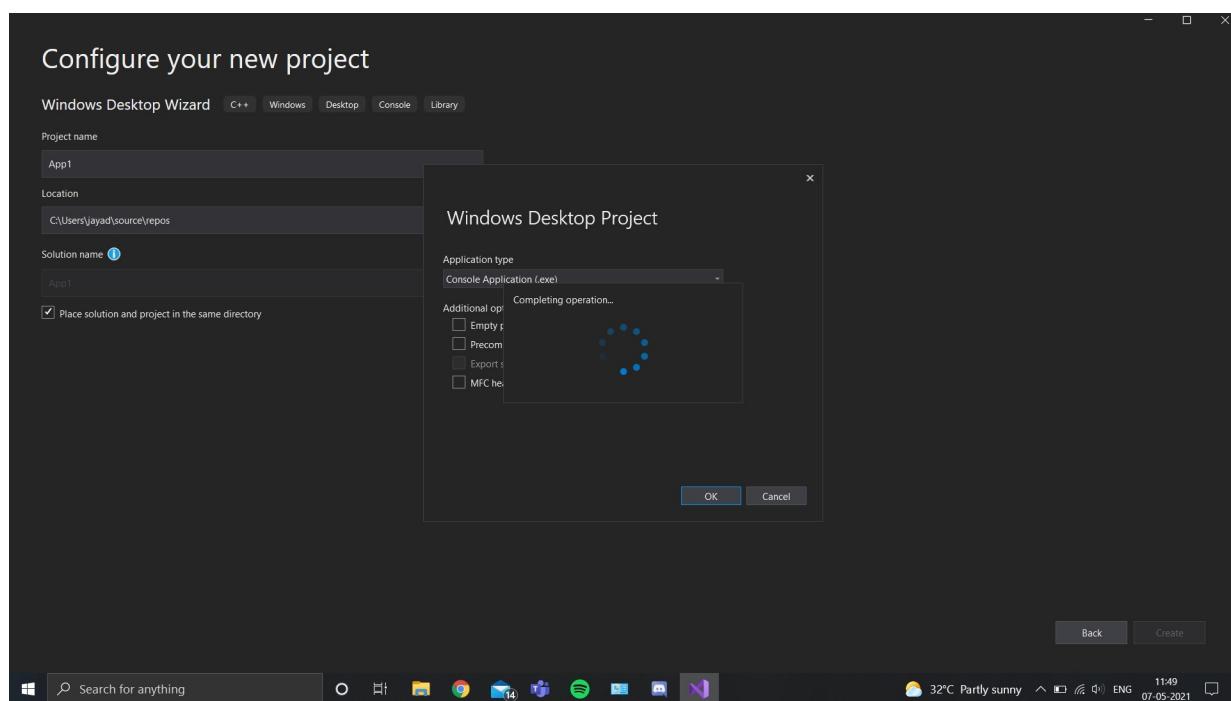


SECURE CODING LAB CSE-2010

LAB-11

Name - Vishal Dung Dung
Reg no - 18BCN7053
Slot - L23-L24

After the installation of Visual Studio :



Generating .exe

SecureCodingApp.cpp

```
SecureCodingApp : Defines the entry point for the application.

// Global Variables:
HINSTANCE hinst; // current instance
WCHAR szTitle[MAX_LOADSTRING]; // The title bar text
WCHAR szWindowClass[MAX_LOADSTRING]; // the main window class name

// Forward declarations of functions included in this code module:
ATOM MyRegisterClass(HINSTANCE hInstance);
BOOL InitInstance(HINSTANCE, int);
LRESULT CALLBACK WndProc(HWND, UINT, WPARAM, LPARAM);
INT_PTR CALLBACK About(HWND, UINT, WPARAM, LPARAM);

int APIENTRY wWinMain(_In_ HINSTANCE hInstance,
                     _In_opt_ HINSTANCE hPrevInstance,
                     _In_ LPWSTR lpCmdLine,
                     _In_ int nCmdShow)
{
    UNREFERENCED_PARAMETER(hPrevInstance);
    UNREFERENCED_PARAMETER(lpCmdLine);

    // TODO: Place code here.
}
```

Output:

```
Show output from: Build
Build started...
1>---- Build started: Project: SecureCodingApp, Configuration: Debug Win32 ----
1>SecureCodingApp.cpp
1>SecureCodingApp.vcxproj -> C:\Users\jayad\source\repos\SecureCodingApp\Debug\SecureCodingApp.exe
----- Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped -----
```

Solution Explorer

Properties

SecureCodingApp Project Properties

(Name) SecureCodingApp

Project Dependencies

Project File C:\Users\jayad\source\repos\SecureCodingApp\SecureCodingApp.vcxproj

Root Namespace SecureCodingApp

(Name)

Specifies the project name.

Package Manager Console

Build succeeded

Disabling DER and ASLR

SecureCodingApp Property Pages

Configuration: Active(Debug) Platform: Active(Win32)

Linker

Output File: No (/NXCOMPAT)

OK Cancel Apply

SecureCodingApp : Defines the entry point for the application.

// Global Variables:
HINSTANCE hinst; // current instance
WCHAR szTitle[MAX_LOADSTRING]; // The title bar text
WCHAR szWindowClass[MAX_LOADSTRING]; // the main window class name

// Forward declarations of functions included in this code module:
ATOM MyRegisterClass(HINSTANCE hInstance);
BOOL InitInstance(HINSTANCE, int);
LRESULT CALLBACK WndProc(HWND, UINT, WPARAM, LPARAM);
INT_PTR CALLBACK About(HWND, UINT, WPARAM, LPARAM);

int APIENTRY wWinMain(_In_ HINSTANCE hInstance,
 _In_opt_ HINSTANCE hPrevInstance,
 In LPWSTR lpCmdLine,
 In int nCmdShow)
{
 UNREFERENCED_PARAMETER(hPrevInstance);
 UNREFERENCED_PARAMETER(lpCmdLine);

 // TODO: Place code here.
}

Output:

```
Show output from: Build
Build started...
1>---- Build started: Project: SecureCodingApp, Configuration: Debug Win32 ----
1>SecureCodingApp.cpp
1>SecureCodingApp.vcxproj -> C:\Users\jayad\source\repos\SecureCodingApp\Debug\SecureCodingApp.exe
----- Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped -----
```

Solution Explorer

Properties

SecureCodingApp Project Properties

(Name) SecureCodingApp

Project Dependencies

Project File C:\Users\jayad\source\repos\SecureCodingApp\SecureCodingApp.vcxproj

Root Namespace SecureCodingApp

(Name)

Specifies the project name.

Package Manager Console

Build succeeded

SecureCodingApp.cpp

```

// SecureCodingApp.cpp : Defines the entry point for the application.

#include "framework.h"
#include "SecureCodingApp.h"

#define MAX_LOADSTRING 100

// Global Variables:
HINSTANCE hInst;
WCHAR szTitle[MAX_LOADSTRING];
WCHAR szWindowClass[MAX_LOADSTRING];

// Forward declarations of functions in
ATOM MyRegisterClass(HINSTANCE hInst, _In_opt_ HINSTANCE hPrevInstance, _In_ LPVOID lpCreateParams);
BOOL InitInstance(HINSTANCE hInst, int nCmdShow);

int APIENTRY wWinMain(_In_ HINSTANCE hInst, _In_opt_ HINSTANCE hPrevInstance, _In_ LPWSTR lpCmdLine, _In_ int nCmdShow)
{
    // ...
}

```

Output

```

Show output from: Build
Build started...
1>----- Build started: Project: SecureCodingApp, Configuration: Debug Win32 -----
1>SecureCodingApp.cpp
1>SecureCodingApp.vcxproj -> C:\Users\jayad\source\repos\SecureCodingApp\SecureCodingApp\SecureCodingApp.vcxproj
----- Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped -----

```

SecureCodingApp Property Pages

Configuration: Active(Debug) Platform: Active(Win32)

Linker

- General
- Input
- Manifest File
- Debugging
- System
- Optimization
- Embedded IDL
- Windows Metadata
- Advanced
- All Options
- Command Line
- Manifest Tool
- Resources
- XML Document Generat
- Browse Information
- Build Events

Output File

The /OUT option overrides the default name and location of the program that the linker creates.

OK Cancel Apply

Solution Explorer

SecureCodingApp

Properties

(Name) SecureCodingApp

Project Dependencies

Project File C:\Users\jayad\source\repos\SecureCodingApp\SecureCodingApp.vcxproj

Root Namespace SecureCodingApp

(Name) Specifies the project name.

SecureCodingApp

Properties

(Name) SecureCodingApp

Project Dependencies

Project File C:\Users\jayad\source\repos\SecureCodingApp\SecureCodingApp.vcxproj

Root Namespace SecureCodingApp

(Name) Specifies the project name.

SecureCodingApp

Properties

(Name) SecureCodingApp

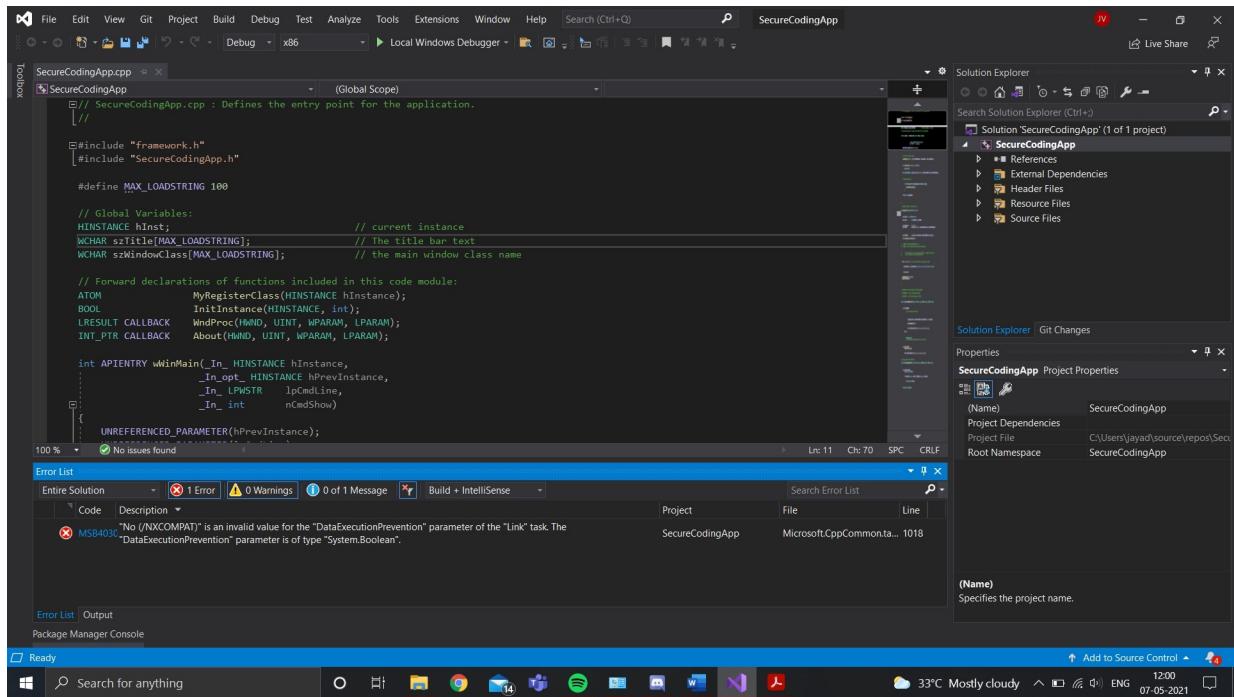
Project Dependencies

Project File C:\Users\jayad\source\repos\SecureCodingApp\SecureCodingApp.vcxproj

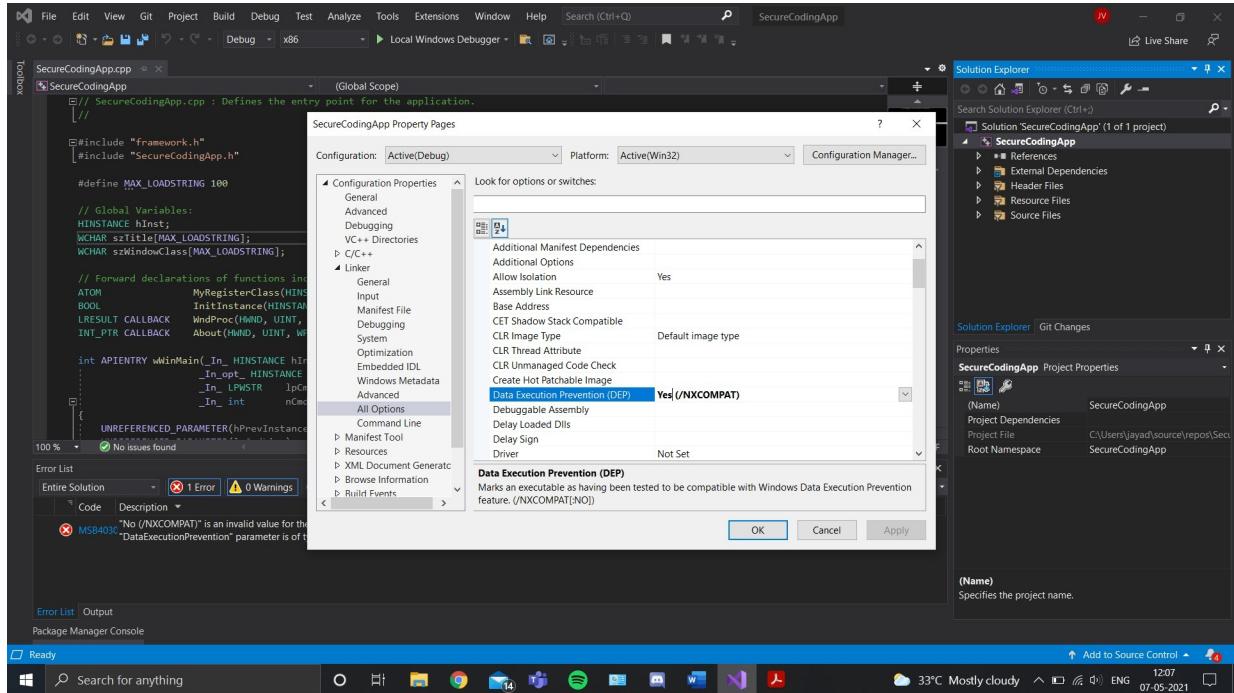
Root Namespace SecureCodingApp

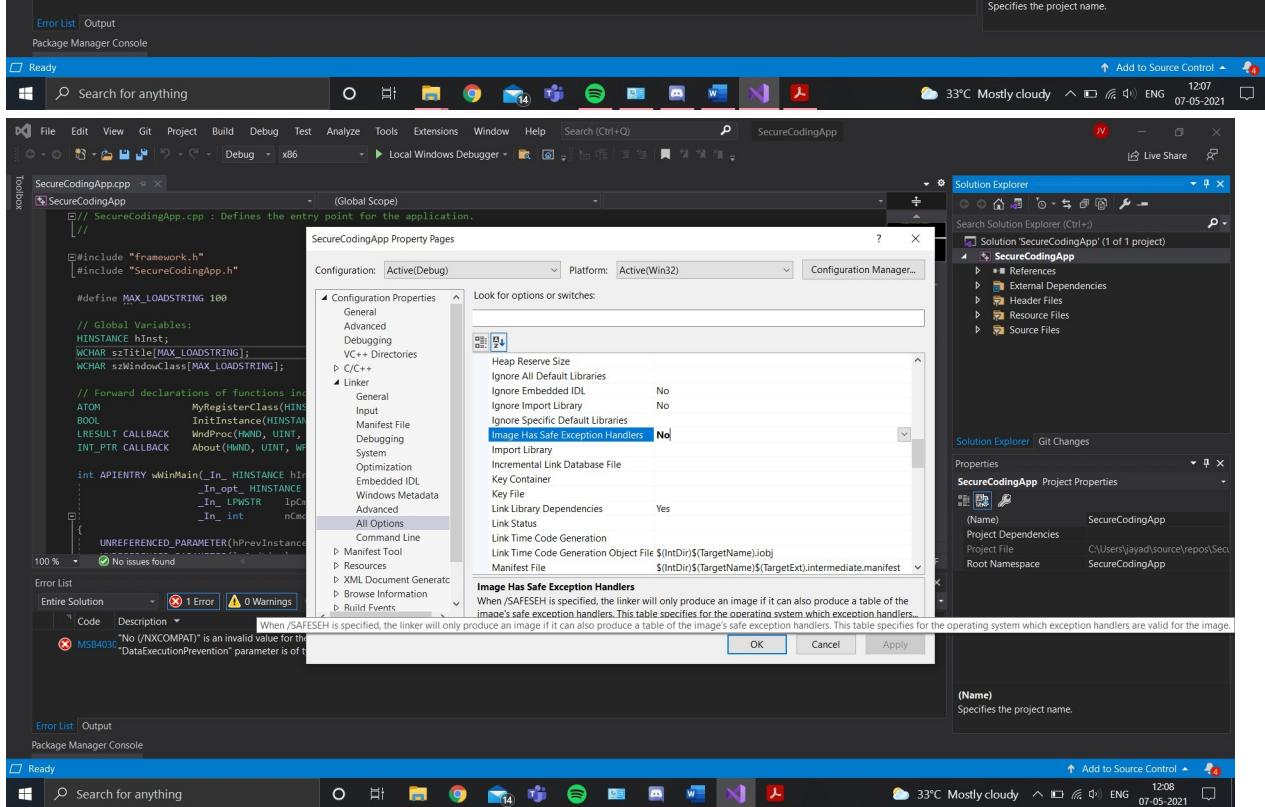
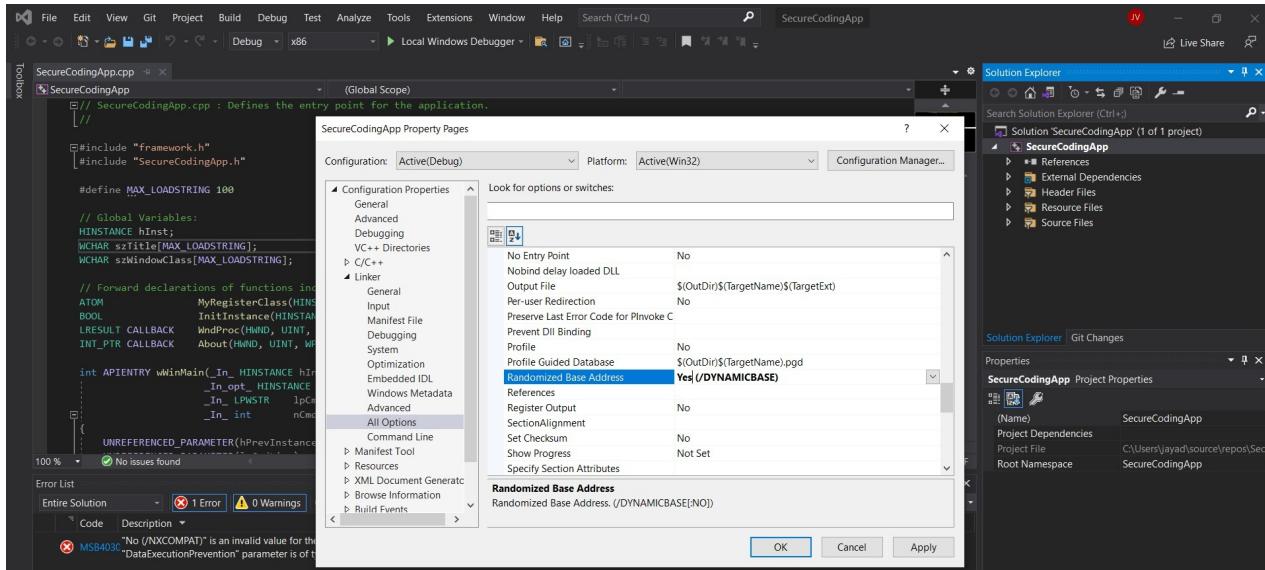
(Name) Specifies the project name.

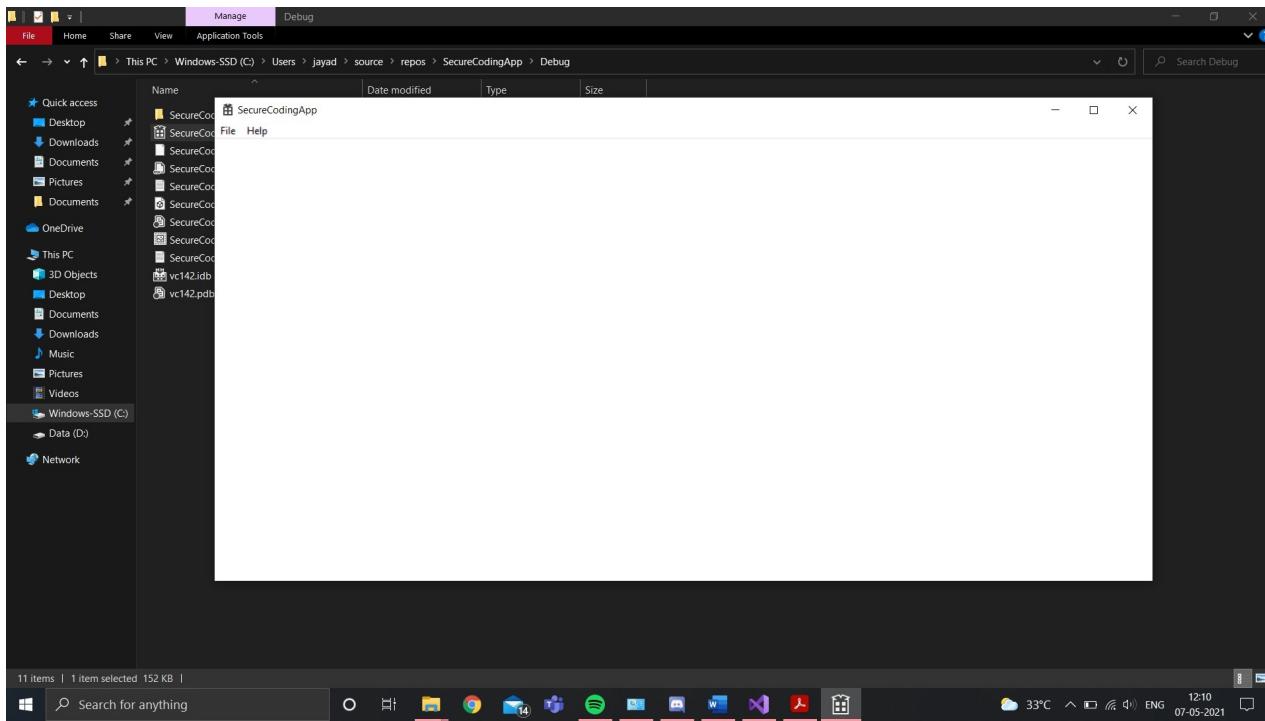
.exe file not created



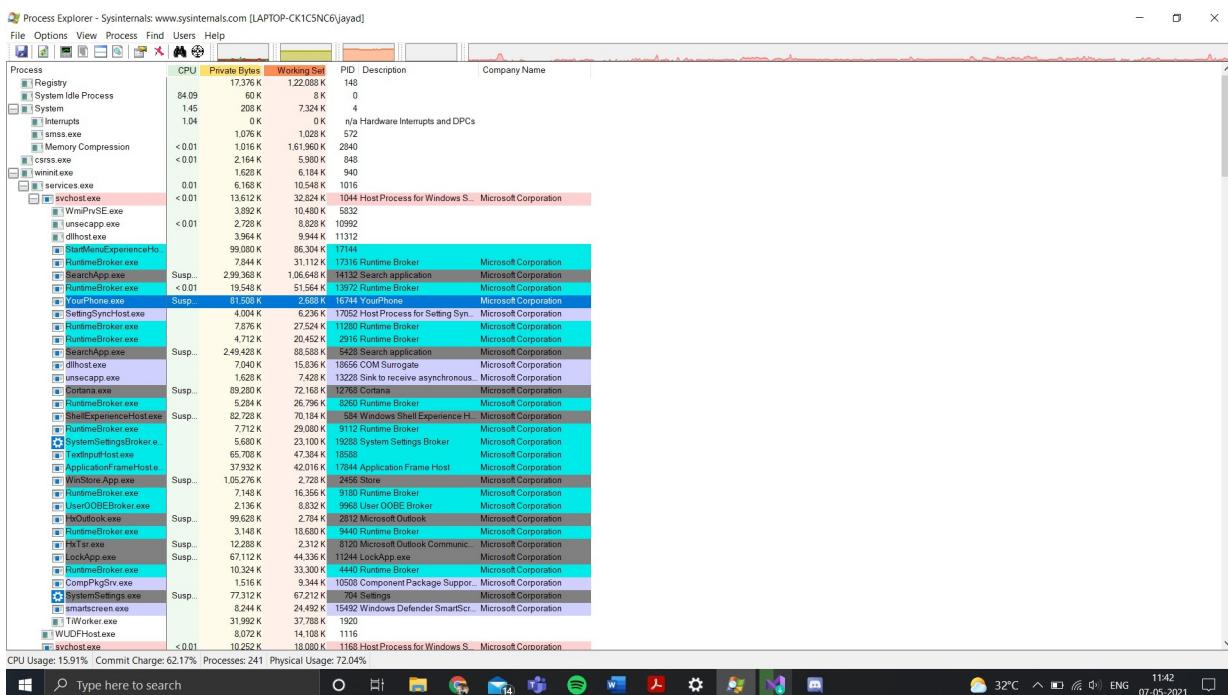
After enabling and running the app







Downloading, installing and analysing through Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-CK1C5NC6\jayad]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
SearchProtocolHost.exe	1.884 K	8.380 K	15976 Microsoft Windows Search Pr.	Microsoft Corporation		
svchost.exe	10.608 K	20.176 K	11992 Host Process for Windows S.	Microsoft Corporation		
SecurityHealthService.exe	3.872 K	13.648 K	9772 Windows Security Health Ser.	Microsoft Corporation		
svchost.exe	2.456 K	10.372 K	11724 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	1.440 K	5.572 K	12016 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	4.772 K	10.164 K	12088 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	2.004 K	11.120 K	12104 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	2.332 K	13.404 K	12404 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	6.864 K	20.236 K	13228 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	3.052 K	11.776 K	13548 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	1.844 K	7.432 K	9172 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	5.300 K	17.624 K	632 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	6.036 K	22.632 K	13852 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	3.400 K	15.184 K	13884 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	3.500 K	11.672 K	22336 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	9.044 K	12.104 K	16352 Host Process for Windows S.	Microsoft Corporation		
SqmBroker.exe	6.372 K	8.332 K	14556 System Guard Runtime Monit.	Microsoft Corporation		
svchost.exe	2.908 K	11.572 K	5340 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	5.060 K	22.572 K	12084 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	3.356 K	11.380 K	2216 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	4.328 K	15.316 K	12504 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	1.784 K	7.768 K	8804 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	3.500 K	11.672 K	22336 Host Process for Windows S.	Microsoft Corporation		
svchost.exe	9.044 K	12.072 K	1016 Local Security Authority Proc.	Microsoft Corporation		
lsass.exe	1.468 K	2.576 K	1036			
fondrvhost.exe	2.658 K	11.656 K	11996			
winlogon.exe	4.224 K	7.076 K	1292			
fontdrvhost.exe	0.27	1.24336 K	67.652 K	1360		
explorer.exe	2.71424 K	23.1028 K	7656 Windows Explorer	Microsoft Corporation		
SecurityHealthStray.exe	< 0.01	1.196 K	9.364 K	Security Health Stray notification.	Microsoft Corporation	
RikAudJUService64.exe	2.348 K	10.144 K	2289 RikAudJU Host Audio Universal...	Realtek Semiconductor		
vtray.exe	< 0.01	1.340 K	6.492 K	4388 Vtray guard tray notification.	Riot Games, Inc.	
OneDrive.exe	0.01	41.263 K	50.800 K	12308 Microsoft OneDrive	Microsoft Corporation	
utility.exe	3.392 K	13.352 K	13056 This utility controls special ke...	Lenovo Group Ltd.		
WINWORD.EXE	1.32916 K	1.38.880 K	2928 Microsoft Word	Microsoft Corporation		
WINWORD.EXE	0.01	1.26.256 K	11.32.72 K	2724 Microsoft Word	Microsoft Corporation	
DevEnv.exe	0.51	3.15.116 K	399.000 K	18048 Microsoft Visual Studio 2019	Microsoft Corporation	
PerWatson2.exe	0.02	48.936 K	69.784 K	11292 PerWatson2	Microsoft Corporation	
MicrosoftServiceHub.Cont...	< 0.01	42.568 K	57.976 K	2624 Microsoft ServiceHub Control.	Microsoft	
ServiceHub.IdentityHost...	< 0.01	75.132 K	83.920 K	13432 ServiceHub.IdentityHost.exe	Microsoft	
ServiceHub.VSDetour...	< 0.01	14.392 K	78.512 K	13744 ServiceHub.VSDetourd!f...	Microsoft	
ServiceHub.SettingsHos...	< 0.01	1.51.612 K	1.05.912 K	17228 ServiceHub.SettingsHost.exe	Microsoft	
ServiceHub.Threaddw...	< 0.01	76.324 K	81.532 K	6732 ServiceHub.Threaddw!WaitDi...	Microsoft	
ServiceHub.ThreadedW...	< 0.01	95.324 K	91.528 K	6732 ServiceHub.Threaddw!WaitDi...	Microsoft	
ServiceHub.HostCLRx8...	< 0.01	1.85.830 K	83.028 K	6056 ServiceHub.HostCLR.x86	Microsoft	
ServiceHub.TestWind...	< 0.01	62.640 K	73.420 K	864 ServiceHub.TestWindowStor...	Microsoft	

CPU Usage: 11.72% Commit Charge: 62.07% Processes: 234 Physical Usage: 71.29%

33°C ENG 12:15 07-05-2021

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-CK1C5NC6\jayad]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
SearchProtocolHost.exe	1.884 K	8.412 K	15976 Microsoft Windows Search Pr.	Microsoft Corporation		
svchost.exe	< 0.01	10.352 K	20.140 K	11992 Host Process for Windows S.	Microsoft Corporation	
SecurityHealthService.exe	1.840 K	10.140 K	9772 Windows Security Health Ser.	Microsoft Corporation		
devenv.exe:18049 Properties	n/a	n/a	n/a	n/a	Microsoft Visual Studio 2019	Microsoft Corporation
svchost.exe	1.840 K	9.364 K	9.364 K	9.364 K	Security Health Stray notification.	Microsoft Corporation
svchost.exe	1.840 K	10.144 K	10.144 K	10.144 K	2289 RikAudJU Host Audio Universal...	Realtek Semiconductor
svchost.exe	1.840 K	11.380 K	6.492 K	6.492 K	4388 Vtray guard tray notification.	Riot Games, Inc.
svchost.exe	1.840 K	13.352 K	13.352 K	13.352 K	13056 This utility controls special ke...	Lenovo Group Ltd.
explorer.exe	2.71424 K	23.1028 K	7656 Windows Explorer	Microsoft Corporation		
SecurityHealthStray.exe	< 0.01	1.196 K	9.364 K	9.364 K	Security Health Stray notification.	Microsoft Corporation
RikAudJUService64.exe	2.348 K	10.144 K	2289 RikAudJU Host Audio Universal...	Realtek Semiconductor		
vtray.exe	< 0.01	1.340 K	6.492 K	6.492 K	4388 Vtray guard tray notification.	Riot Games, Inc.
OneDrive.exe	0.01	41.263 K	50.800 K	12308 Microsoft OneDrive	Microsoft Corporation	
utility.exe	3.392 K	13.352 K	13.352 K	13.352 K	13056 This utility controls special ke...	Lenovo Group Ltd.
WINWORD.EXE	1.32916 K	1.38.880 K	2928 Microsoft Word	Microsoft Corporation		
WINWORD.EXE	0.01	1.26.256 K	11.32.72 K	2724 Microsoft Word	Microsoft Corporation	
DevEnv.exe	0.51	3.15.116 K	399.000 K	18048 Microsoft Visual Studio 2019	Microsoft Corporation	
PerWatson2.exe	0.02	48.936 K	69.784 K	11292 PerWatson2	Microsoft Corporation	
MicrosoftServiceHub.Cont...	< 0.01	42.568 K	57.976 K	2624 Microsoft ServiceHub Control.	Microsoft	
ServiceHub.IdentityHost...	< 0.01	75.132 K	83.920 K	13432 ServiceHub.IdentityHost.exe	Microsoft	
ServiceHub.VSDetour...	< 0.01	14.392 K	78.512 K	13744 ServiceHub.VS!Detourd!f...	Microsoft	
ServiceHub.SettingsHos...	< 0.01	1.51.612 K	1.05.912 K	17228 ServiceHub.SettingsHost.exe	Microsoft	
ServiceHub.Threaddw...	< 0.01	76.324 K	81.532 K	6732 ServiceHub.Threaddw!WaitDi...	Microsoft	
ServiceHub.ThreadedW...	< 0.01	95.324 K	91.528 K	6732 ServiceHub.Threaddw!WaitDi...	Microsoft	
ServiceHub.HostCLRx8...	< 0.01	1.85.830 K	83.028 K	6056 ServiceHub.HostCLR.x86	Microsoft	
ServiceHub.TestWind...	< 0.01	62.640 K	73.420 K	864 ServiceHub.TestWindowStor...	Microsoft	

CPU Usage: 12.20% Commit Charge: 62.25% Processes: 234 Physical Usage: 71.93%

33°C ENG 12:15 07-05-2021