# LAB 11

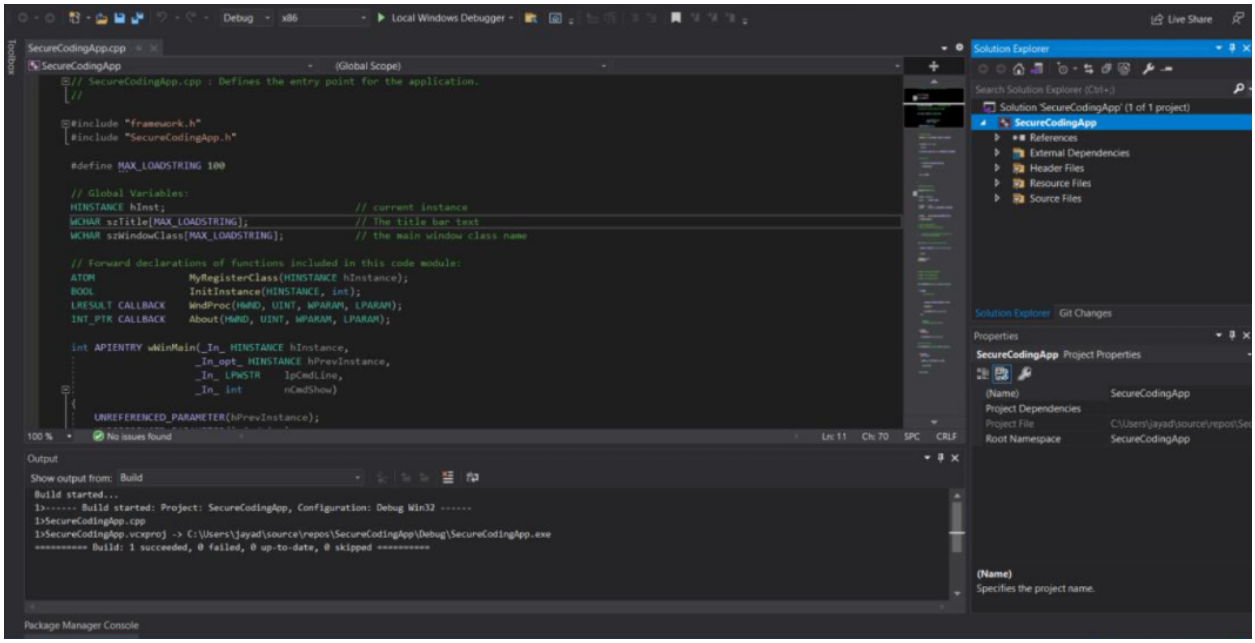
K.SIVA KARTHIK
19BCE7416

---

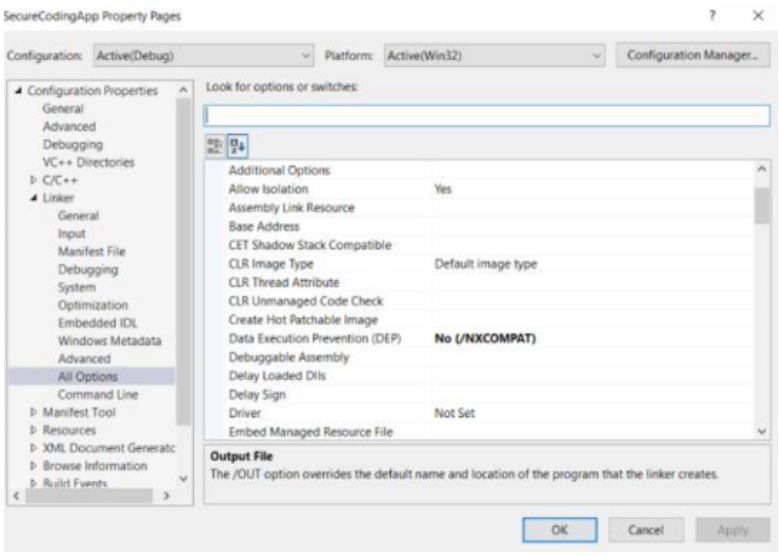
**Lab experiment – Creating secure and safe executable**

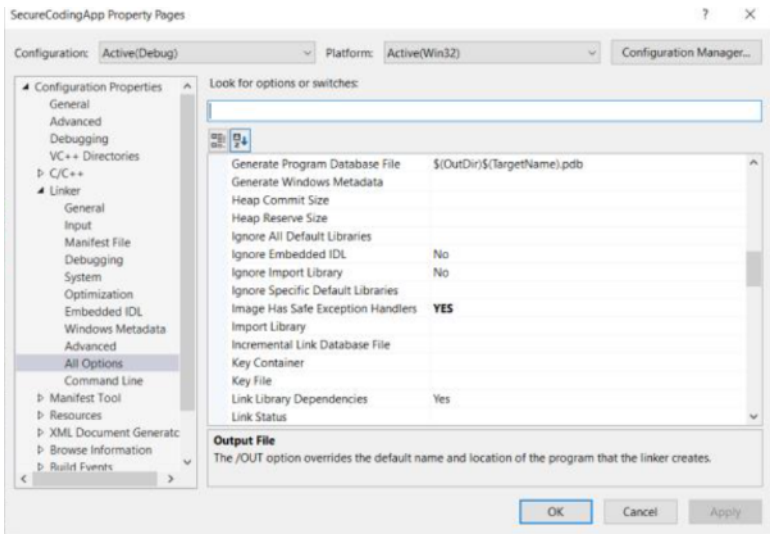
**Download and install visual studio (recent edition)**
**Write a C++ code of your own to build an executable and run the same.**
**Download process explorer and verify the DEP & ASLR status**
**Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable**
**Again, verify the DEP & ASLR status in the process explorer**
**Report the same with separate screenshot - before and after enabling DEP & ASLR.**

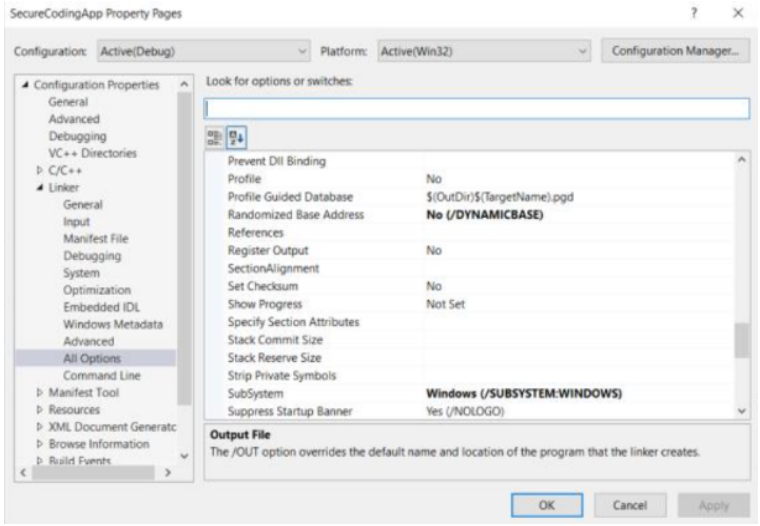
- **Create a new executable (.exe) file.**



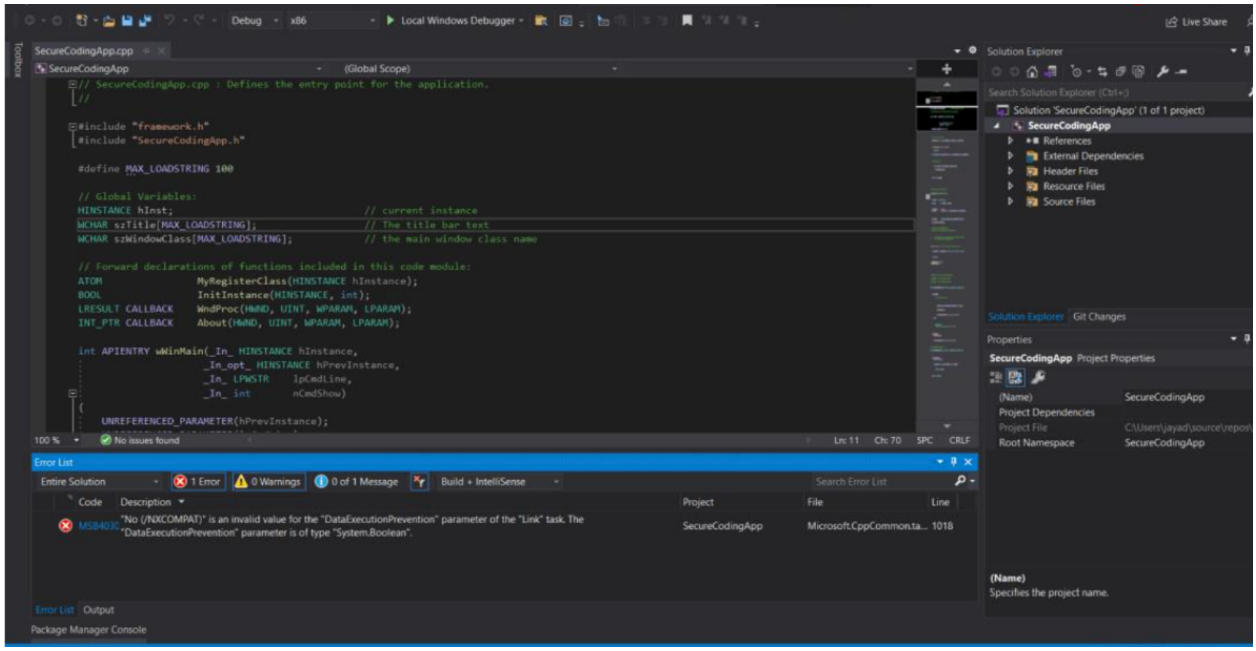

- **Disabling DER and ASLR.**


SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generatc
Browse Information
Build Events
Look for options or switches:
Additional Options
Allow Isolation Yes
Assembly Link Resource
Base Address
CET Shadow Stack Compatible
CLR Image Type Default image type
CLR Thread Attribute
CLR Unmanaged Code Check
Create Hot Patchable Image
Data Execution Prevention (DEP) No (/NXCOMPAT)
Debuggable Assembly
Delay Loaded Dlls
Delay Sign
Driver Not Set
Embed Managed Resource File
Output File
The /OUT option overrides the default name and location of the program that the linker creates.
OK
Cancel
Apply

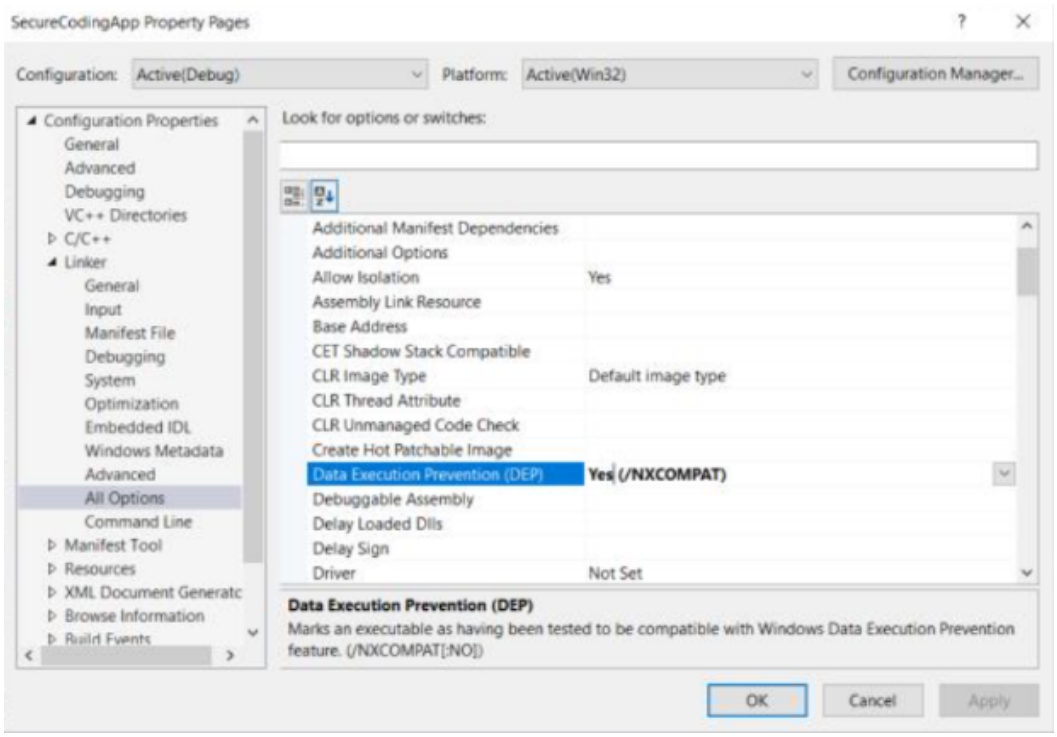

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generatc
Browse Information
Build Events
Look for options or switches:
Generate Program Database File $(OutDir)$(TargetName).pdb
Generate Windows Metadata
Heap Commit Size
Heap Reserve Size
Ignore All Default Libraries
Ignore Embedded IDL No
Ignore Import Library No
Ignore Specific Default Libraries
Image Has Safe Exception Handlers YES
Import Library
Incremental Link Database File
Key Container
Key File
Link Library Dependencies Yes
Link Status
Output File
The /OUT option overrides the default name and location of the program that the linker creates.
OK
Cancel
Apply

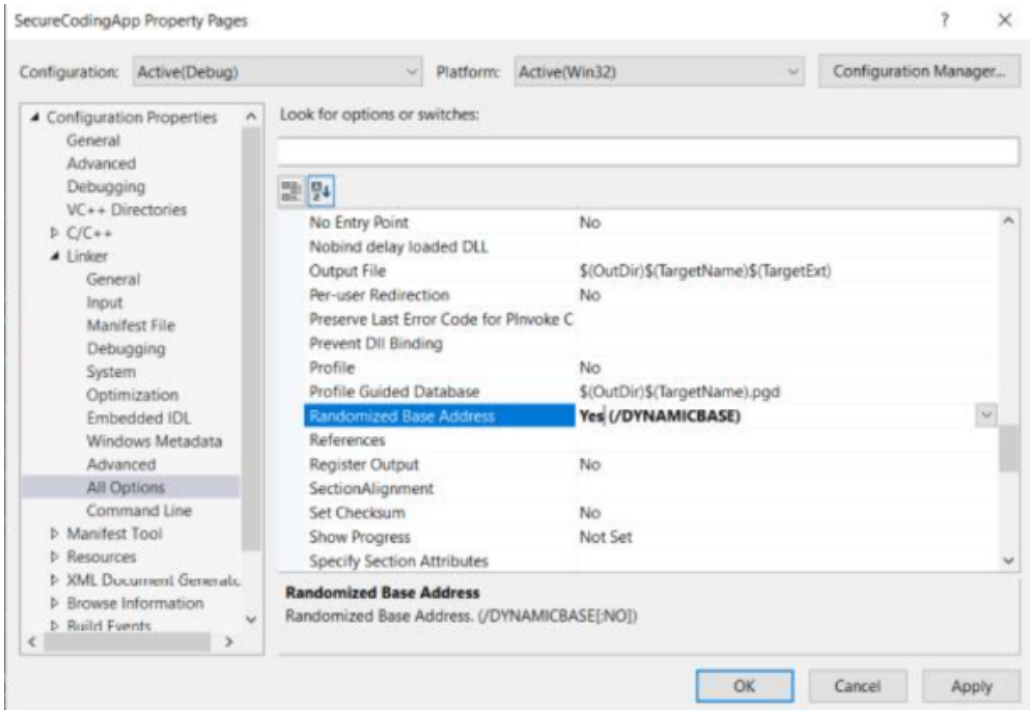

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generatc
Browse Information
Build Events
Look for options or switches:
Prevent Dll Binding
Profile No
Profile Guided Database $(OutDir)$(TargetName).pgd
Randomized Base Address No (/DYNAMICBASE)
References
Register Output No
SectionAlignment
Set Checksum No
Show Progress Not Set
Specify Section Attributes
Stack Commit Size
Stack Reserve Size
Strip Private Symbols
SubSystem Windows (/SUBSYSTEM:WINDOWS)
Suppress Startup Banner Yes (/NOLOGO)
Output File
The /OUT option overrides the default name and location of the program that the linker creates.
OK
Cancel
Apply

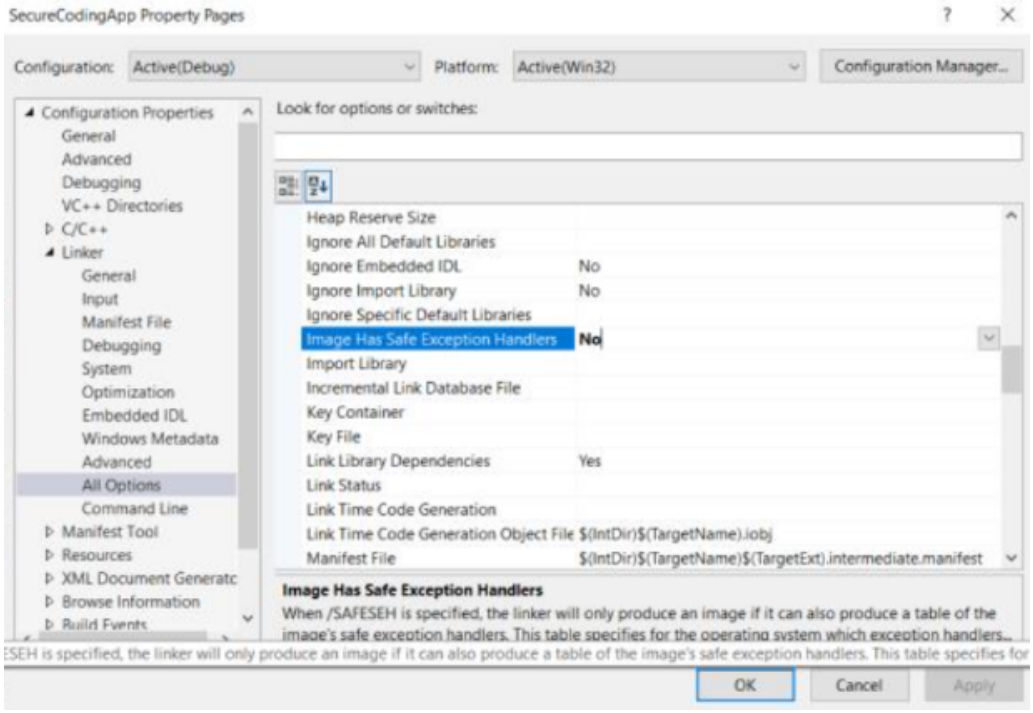
## Executable (.exe) file not created.



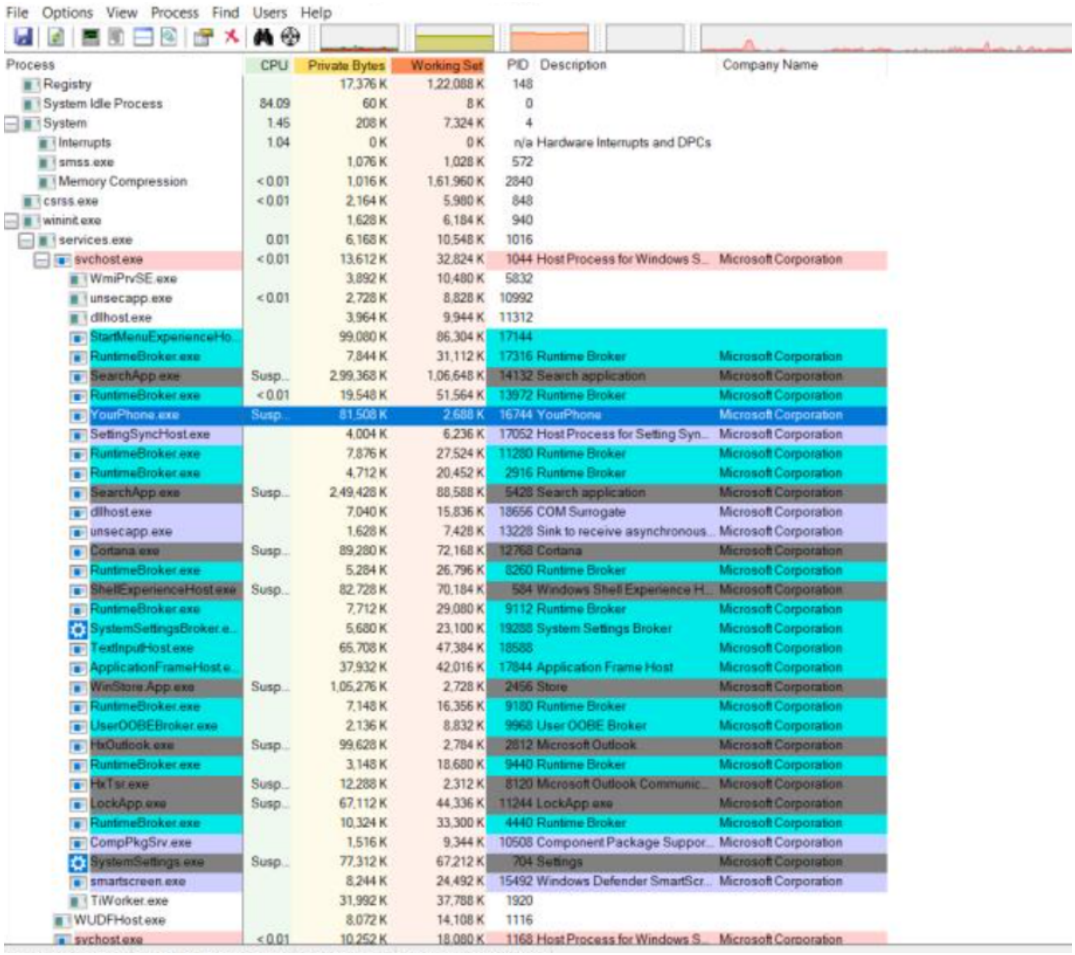

## Enabling and Running the application.




SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generato
Browse Information
Build Events
Look for options or switches:
No Entry Point No
Nobind delay loaded DLL
Output File $(OutDir)$(TargetName)$(TargetExt)
Per-user Redirection No
Preserve Last Error Code for PInvoke C
Prevent Dll Binding
Profile No
Profile Guided Database $(OutDir)$(TargetName).pgd
Randomized Base Address Yes (/DYNAMICBASE)
References
Register Output No
SectionAlignment
Set Checksum No
Show Progress Not Set
Specify Section Attributes
Randomized Base Address
Randomized Base Address. (/DYNAMICBASE[:NO])
OK
Cancel
Apply

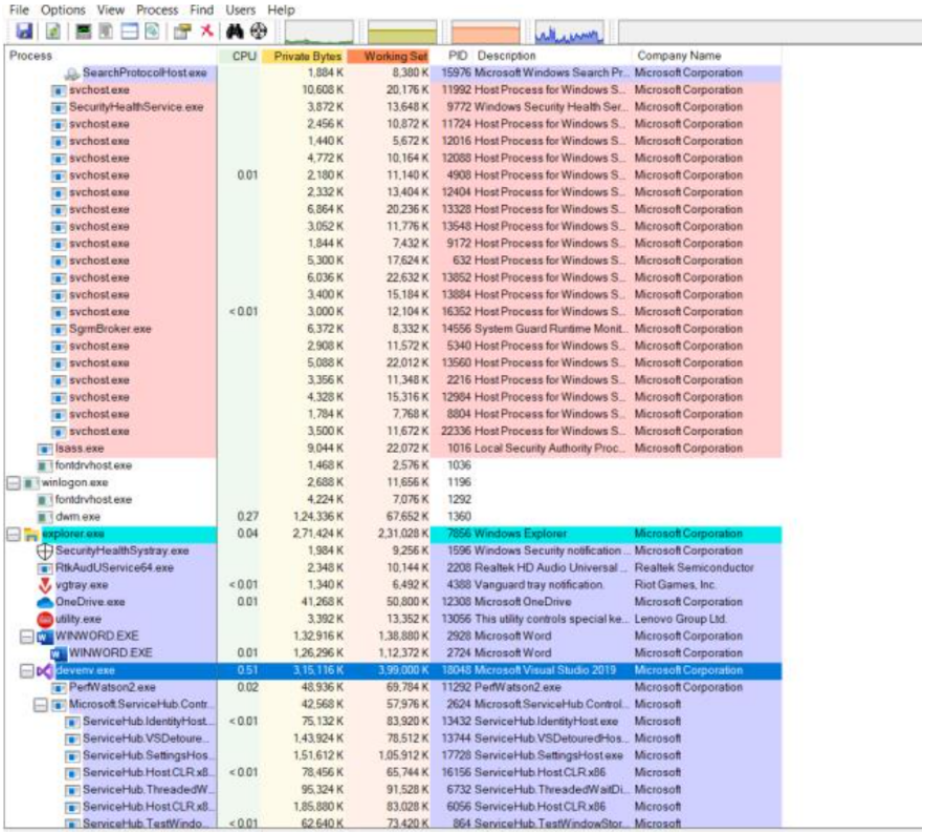

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generatc
Browse Information
Build Events
Look for options or switches:
Heap Reserve Size
Ignore All Default Libraries
Ignore Embedded IDL No
Ignore Import Library No
Ignore Specific Default Libraries
Image Has Safe Exception Handlers No
Import Library
Incremental Link Database File
Key Container
Key File
Link Library Dependencies Yes
Link Status
Link Time Code Generation
Link Time Code Generation Object File $(IntDir)$(TargetName).iobj
Manifest File $(IntDir)$(TargetName)$(TargetExt).intermediate.manifest
Image Has Safe Exception Handlers
When /SAFESEH is specified, the linker will only produce an image if it can also produce a table of the
image's safe exception handlers. This table specifies for the operating system which exception handlers...
ESEH is specified, the linker will only produce an image if it can also produce a table of the image's safe exception handlers. This table specifies for
OK
Cancel
Apply

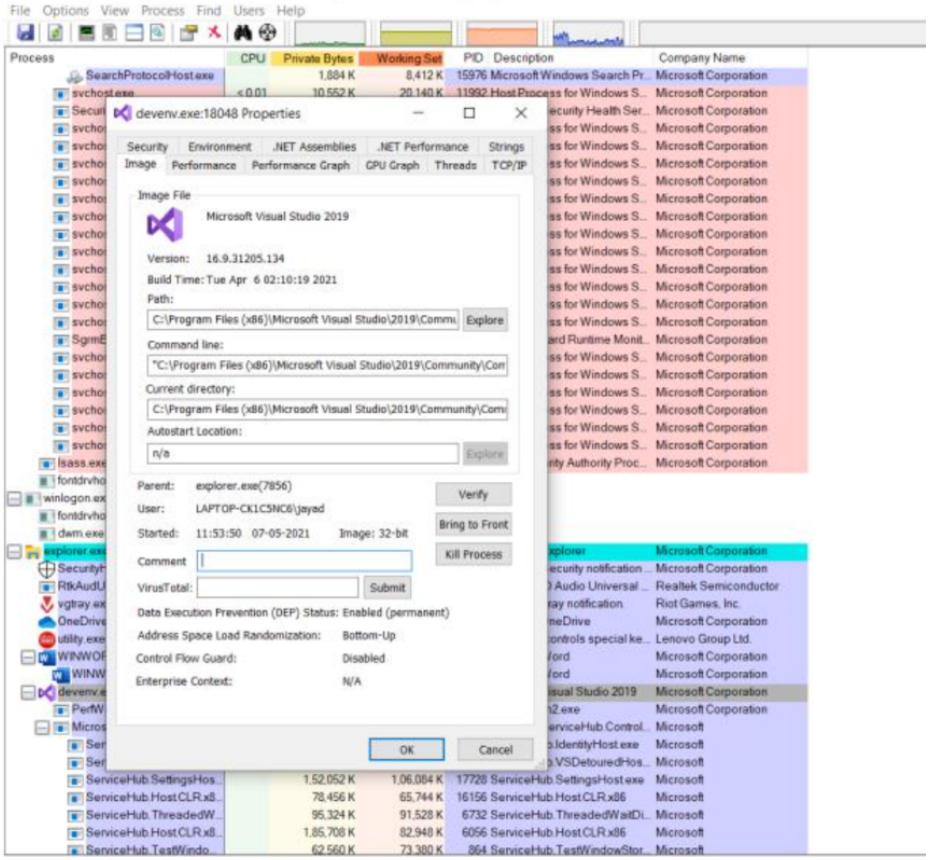
# Downloading ,Installing and Analysing through Process Explorer.



File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|---|---|---|---|---|---|---|
| Registry | | 17,376 K | 1,22,088 K | 148 | | |
| System Idle Process | 84.09 | 60 K | 8 K | 0 | | |
| System | 1.45 | 208 K | 7,324 K | 4 | | |
| Interrupts | 1.04 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 1,076 K | 1,028 K | 572 | | |
| Memory Compression | < 0.01 | 1,016 K | 1,61,960 K | 2840 | | |
| csrss.exe | < 0.01 | 2,164 K | 5,980 K | 848 | | |
| wininit.exe | | 1,628 K | 6,184 K | 940 | | |
| services.exe | 0.01 | 6,168 K | 10,548 K | 1016 | | |
| svchost.exe | < 0.01 | 13,612 K | 32,824 K | 1044 | Host Process for Windows S... | Microsoft Corporation |
| WmiPrvSE.exe | | 3,892 K | 10,480 K | 5832 | | |
| unsecapp.exe | < 0.01 | 2,728 K | 8,828 K | 10992 | | |
| dllhost.exe | | 3,964 K | 9,944 K | 11312 | | |
| StartMenuExperienceHo... | | 99,080 K | 86,304 K | 17144 | | |
| RuntimeBroker.exe | | 7,844 K | 31,112 K | 17316 | Runtime Broker | Microsoft Corporation |
| SearchApp.exe | Susp... | 2,99,368 K | 1,06,648 K | 14132 | Search application | Microsoft Corporation |
| RuntimeBroker.exe | < 0.01 | 19,548 K | 51,564 K | 13972 | Runtime Broker | Microsoft Corporation |
| YourPhone.exe | Susp... | 81,508 K | 2,688 K | 16744 | YourPhone | Microsoft Corporation |
| SettingSyncHost.exe | | 4,004 K | 6,236 K | 17052 | Host Process for Setting Syn... | Microsoft Corporation |
| RuntimeBroker.exe | | 7,876 K | 27,524 K | 11280 | Runtime Broker | Microsoft Corporation |
| RuntimeBroker.exe | | 4,712 K | 20,452 K | 2916 | Runtime Broker | Microsoft Corporation |
| SearchApp.exe | Susp... | 2,49,428 K | 88,588 K | 5428 | Search application | Microsoft Corporation |
| dllhost.exe | | 7,040 K | 15,836 K | 18656 | COM Surrogate | Microsoft Corporation |
| unsecapp.exe | | 1,628 K | 7,428 K | 13228 | Sink to receive asynchronous... | Microsoft Corporation |
| Cortana.exe | Susp... | 89,280 K | 72,168 K | 12768 | Cortana | Microsoft Corporation |
| RuntimeBroker.exe | | 5,284 K | 26,796 K | 8260 | Runtime Broker | Microsoft Corporation |
| ShellExperienceHost.exe | Susp... | 82,728 K | 70,184 K | 584 | Windows Shell Experience H... | Microsoft Corporation |
| RuntimeBroker.exe | | 7,712 K | 29,080 K | 9112 | Runtime Broker | Microsoft Corporation |
| SystemSettingsBroker.e... | | 5,680 K | 23,100 K | 19288 | System Settings Broker | Microsoft Corporation |
| TextInputHost.exe | | 65,708 K | 47,384 K | 18588 | | Microsoft Corporation |
| ApplicationFrameHost.e... | | 37,932 K | 42,016 K | 17844 | Application Frame Host | Microsoft Corporation |
| WinStore.App.exe | Susp... | 1,05,276 K | 2,728 K | 2456 | Store | Microsoft Corporation |
| RuntimeBroker.exe | | 7,148 K | 16,356 K | 9180 | Runtime Broker | Microsoft Corporation |
| UserOOBEBroker.exe | | 2,136 K | 8,832 K | 9968 | User OOBE Broker | Microsoft Corporation |
| HxOutlook.exe | Susp... | 99,628 K | 2,784 K | 2812 | Microsoft Outlook | Microsoft Corporation |
| RuntimeBroker.exe | | 3,148 K | 18,680 K | 9440 | Runtime Broker | Microsoft Corporation |
| HxTsr.exe | Susp... | 12,288 K | 2,312 K | 8120 | Microsoft Outlook Communic... | Microsoft Corporation |
| LockApp.exe | Susp... | 67,112 K | 44,336 K | 11244 | LockApp.exe | Microsoft Corporation |
| RuntimeBroker.exe | | 10,324 K | 33,300 K | 4440 | Runtime Broker | Microsoft Corporation |
| CompPkgSrv.exe | | 1,516 K | 9,344 K | 10508 | Component Package Suppor... | Microsoft Corporation |
| SystemSettings.exe | Susp... | 77,312 K | 67,212 K | 704 | Settings | Microsoft Corporation |
| smartscreen.exe | | 8,244 K | 24,492 K | 15492 | Windows Defender SmartScr... | Microsoft Corporation |
| TiWorker.exe | | 31,992 K | 37,788 K | 1920 | | |
| WUDFHost.exe | | 8,072 K | 14,108 K | 1116 | | |
| svchost.exe | < 0.01 | 10,252 K | 18,080 K | 1168 | Host Process for Windows S... | Microsoft Corporation |


File Options View Process Find Users Help
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 10,872 K 11724 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,440 K 5,672 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 0.01 2,180 K 11,140 K 4908 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 13328 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 < 0.01 3,000 K 12,104 K 16352 Host Process for Windows S... Microsoft Corporation
SgrmBroker.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 5,088 K 22,012 K 13560 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,356 K 11,348 K 2216 Host Process for Windows S... Microsoft Corporation
svchost.exe 4,328 K 15,316 K 12984 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
lsass.exe 9,044 K 22,072 K 1016 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 1,468 K 2,576 K 1036
winlogon.exe 2,688 K 11,656 K 1196
fontdrvhost.exe 4,224 K 7,076 K 1292
dwm.exe 0.27 1,24,336 K 67,652 K 1360
explorer.exe 0.04 2,71,424 K 2,31,028 K 7856 Windows Explorer Microsoft Corporation
SecurityHealthSystray.exe 1,984 K 9,256 K 1596 Windows Security notification ... Microsoft Corporation
RtkAudUService64.exe 2,348 K 10,144 K 2208 Realtek HD Audio Universal ... Realtek Semiconductor
vgtray.exe < 0.01 1,340 K 6,492 K 4388 Vanguard tray notification. Riot Games, Inc.
OneDrive.exe 0.01 41,268 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 1,32,916 K 1,38,880 K 2928 Microsoft Word Microsoft Corporation
WINWORD.EXE 0.01 1,26,296 K 1,12,372 K 2724 Microsoft Word Microsoft Corporation
devenv.exe 0.51 3,15,116 K 3,99,000 K 18048 Microsoft Visual Studio 2019 Microsoft Corporation
PerfWatson2.exe 0.02 48,936 K 69,784 K 11292 PerfWatson2.exe Microsoft Corporation
Microsoft.ServiceHub.Contr... 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.VSDetoure... 1,43,924 K 78,512 K 13744 ServiceHub.VSDetouredHos... Microsoft
ServiceHub.SettingsHos... 1,51,612 K 1,05,912 K 17728 ServiceHub.SettingsHost.exe Microsoft
ServiceHub.Host.CLR.x8... < 0.01 78,456 K 65,744 K 16156 ServiceHub.Host.CLR.x86 Microsoft
ServiceHub.ThreadedW... 95,324 K 91,528 K 6732 ServiceHub.ThreadedWaitDi... Microsoft
ServiceHub.Host.CLR.x8... 1,85,880 K 83,028 K 6056 ServiceHub.Host.CLR.x86 Microsoft
ServiceHub.TestWindo... < 0.01 62,640 K 73,420 K 864 ServiceHub.TestWindowStor... Microsoft


File Options View Process Find Users Help
devenv.exe:18048 Properties
Security Environment .NET Assemblies .NET Performance Strings
Image Performance Performance Graph GPU Graph Threads TCP/IP
Image File
Microsoft Visual Studio 2019
Version: 16.9.31205.134
Build Time: Tue Apr 6 02:10:19 2021
Path:
C:\Program Files (x86)\Microsoft Visual Studio\2019\Comm
Explore
Command line:
"C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Com
Current directory:
C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Com
Autostart Location:
n/a
Explore
Parent: explorer.exe(7856)
User: LAPTOP-CK1C5NC6\jayad
Started: 11:53:50 07-05-2021 Image: 32-bit
Comment
VirusTotal:
Submit
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: Bottom-Up
Control Flow Guard: Disabled
Enterprise Context: N/A
Verify
Bring to Front
Kill Process
OK
Cancel