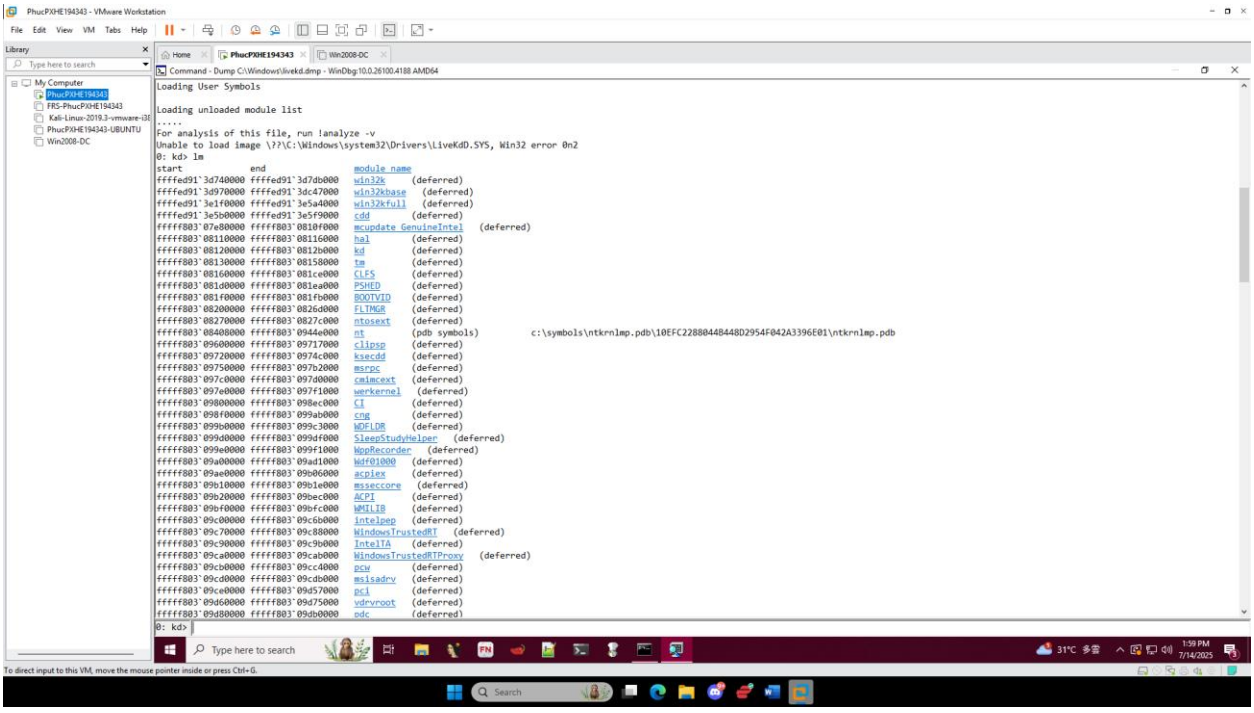
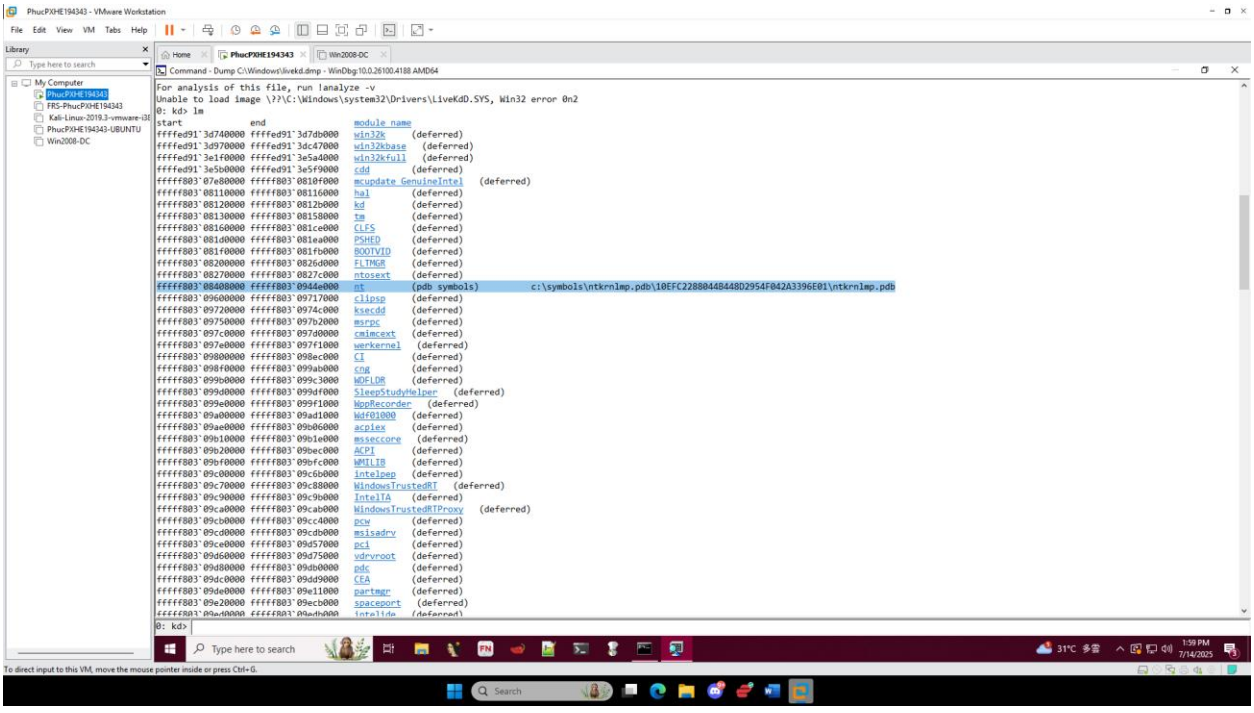
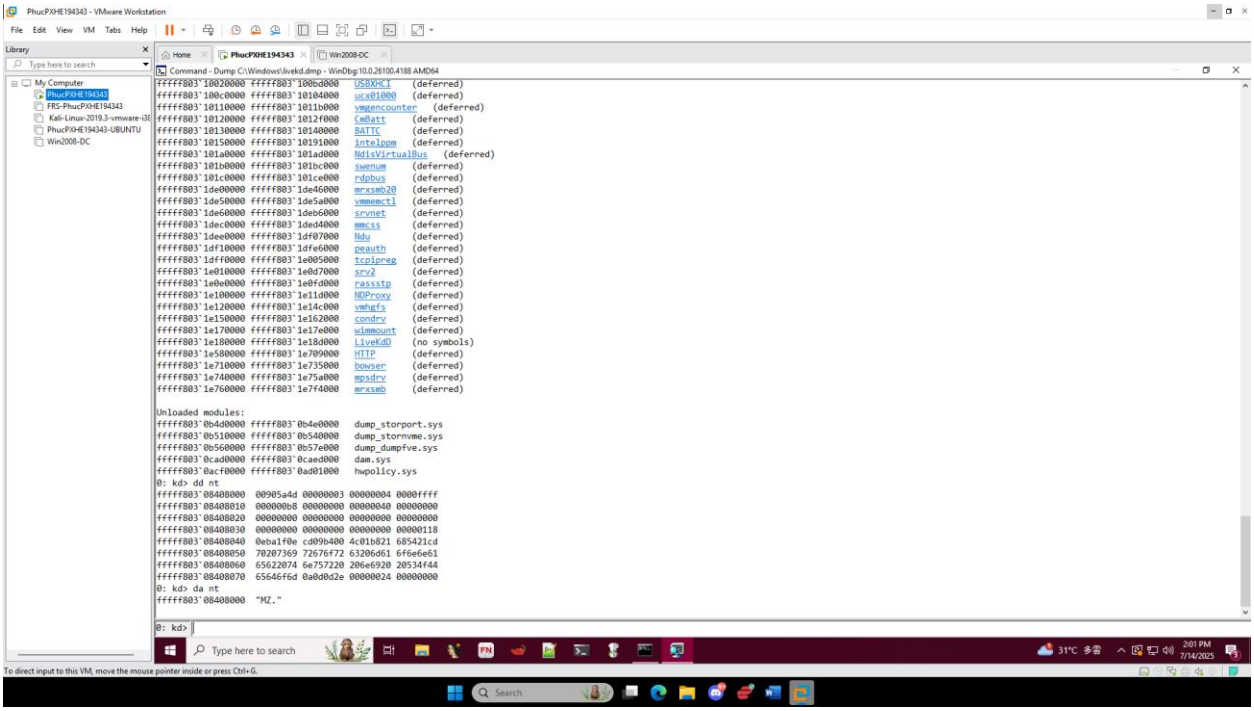
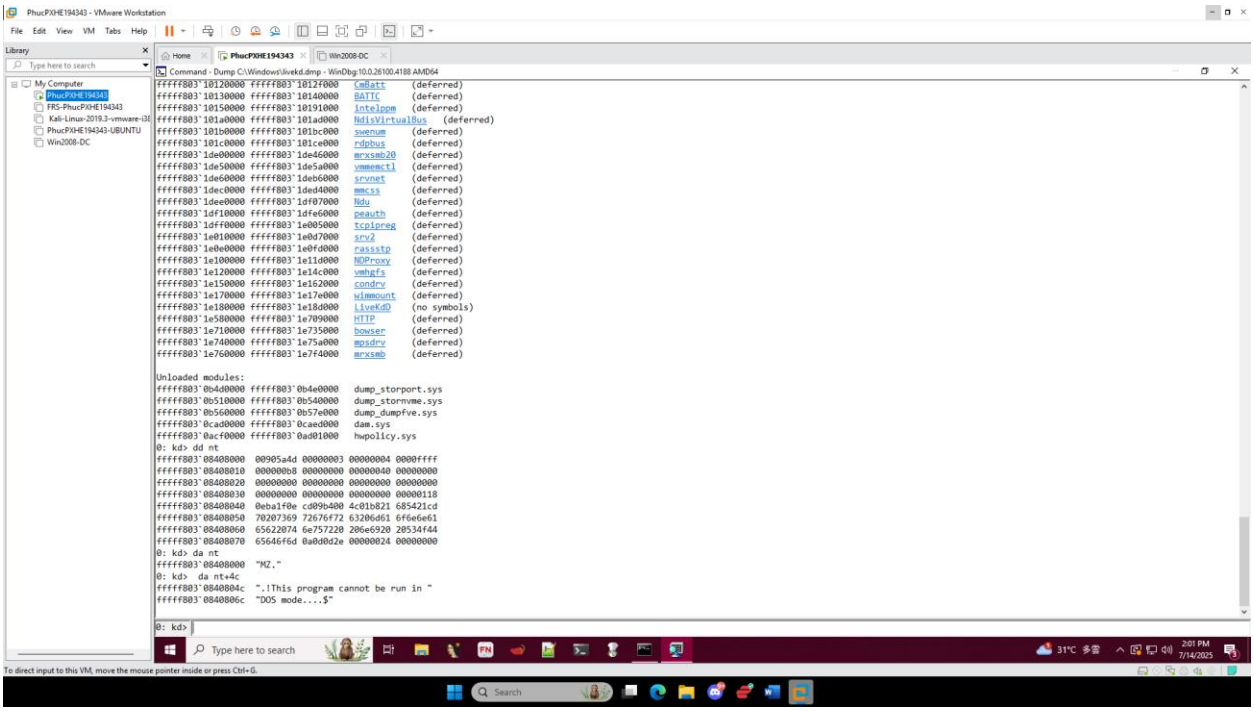
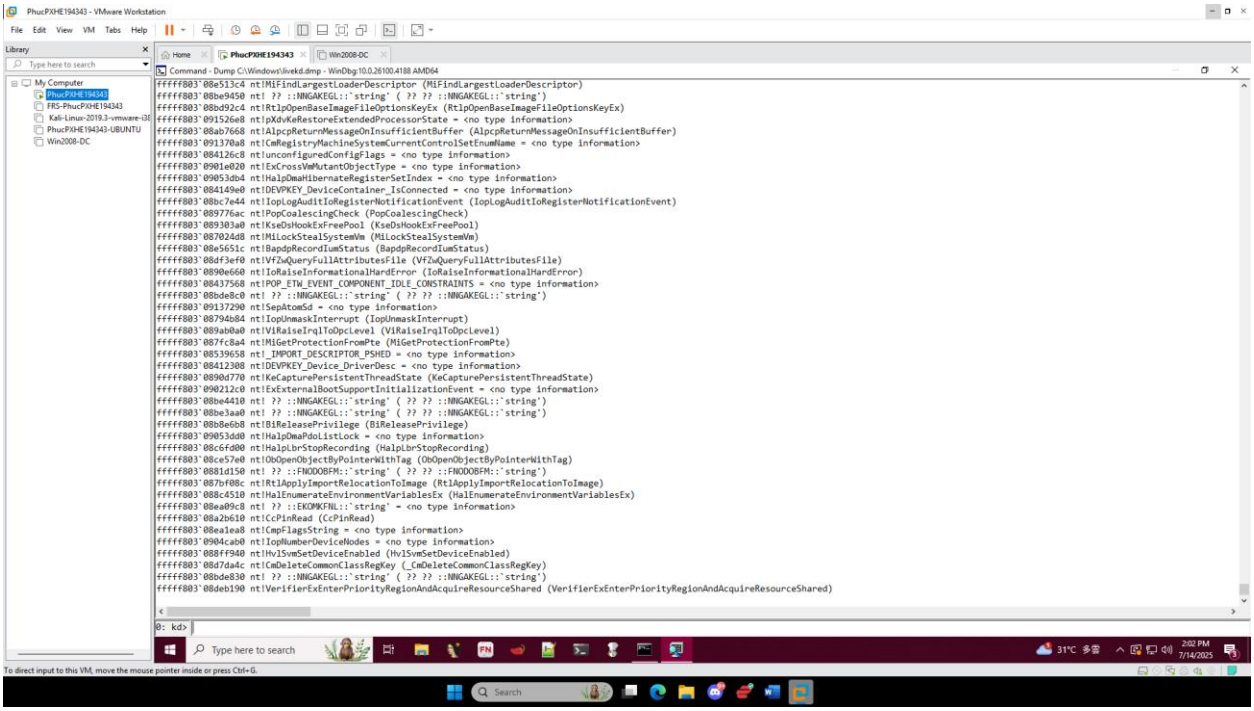
Lab 17

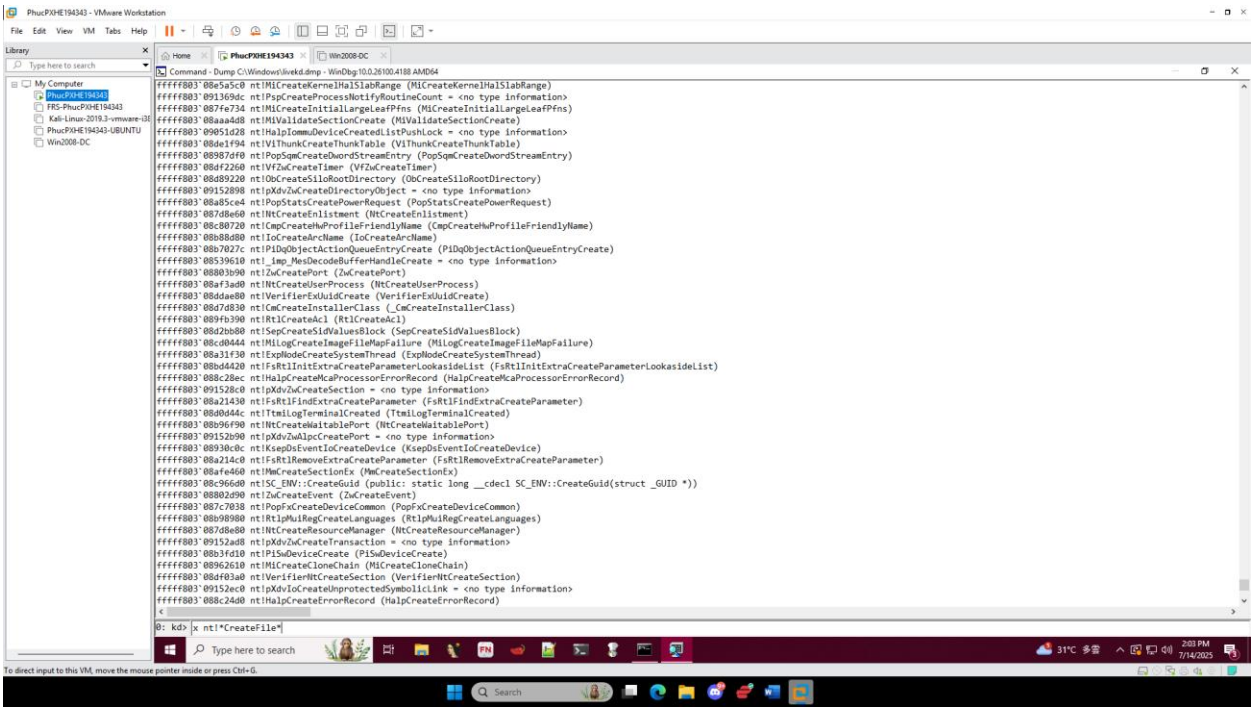

PhucPXHE194343 - VMware Workstation
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
Loading User Symbols
Loading unloaded module list
.....
For analysis of this file, run !analyze -v
Unable to load image \??\C:\Windows\system32\Drivers\LiveKdD.SYS, Win32 error 0n2
0: kd> lm
start end module name
fffed91`3d740000 fffed91`3d7db000 win32k (deferred)
fffed91`3d970000 fffed91`3dc47000 win32kbase (deferred)
fffed91`3e1f0000 fffed91`3e5a4000 win32kfull (deferred)
fffed91`3e5b0000 fffed91`3e5f9000 cdd (deferred)
fffff803`07e80000 fffff803`0810f000 mcupdate_GenuineIntel (deferred)
fffff803`08110000 fffff803`08116000 hal (deferred)
fffff803`08120000 fffff803`0812b000 kd (deferred)
fffff803`08130000 fffff803`08158000 tm (deferred)
fffff803`08160000 fffff803`081ce000 CLFS (deferred)
fffff803`081d0000 fffff803`081ea000 PSHED (deferred)
fffff803`081f0000 fffff803`081fb000 BOOTVID (deferred)
fffff803`08200000 fffff803`0826d000 FLTMGR (deferred)
fffff803`08270000 fffff803`0827c000 ntosext (deferred)
fffff803`08408000 fffff803`0944e000 nt (pdb symbols) c:\symbols\ntkrnlmp.pdb\10EFC2288044B448D2954F042A3396E01\ntkrnlmp.pdb
fffff803`09600000 fffff803`09717000 clipsp (deferred)
fffff803`09720000 fffff803`0974c000 ksecdd (deferred)
fffff803`09750000 fffff803`097b2000 msrpc (deferred)
fffff803`097c0000 fffff803`097d0000 cmimcext (deferred)
fffff803`097e0000 fffff803`097f1000 werkernel (deferred)
fffff803`09800000 fffff803`098ec000 CI (deferred)
fffff803`098f0000 fffff803`099ab000 cng (deferred)
fffff803`099b0000 fffff803`099c3000 WDFLDR (deferred)
fffff803`099d0000 fffff803`099df000 SleepStudyHelper (deferred)
fffff803`099e0000 fffff803`099f1000 WppRecorder (deferred)
fffff803`09a00000 fffff803`09ad1000 Wdf01000 (deferred)
fffff803`09ae0000 fffff803`09b06000 acpiex (deferred)
fffff803`09b10000 fffff803`09b1e000 msseccore (deferred)
fffff803`09b20000 fffff803`09bec000 ACPI (deferred)
fffff803`09bf0000 fffff803`09bfc000 WMILIB (deferred)
fffff803`09c00000 fffff803`09c6b000 intelpep (deferred)
fffff803`09c70000 fffff803`09c88000 WindowsTrustedRT (deferred)
fffff803`09c90000 fffff803`09c9b000 IntelTA (deferred)
fffff803`09ca0000 fffff803`09cab000 WindowsTrustedRTProxy (deferred)
fffff803`09cb0000 fffff803`09cc4000 pcw (deferred)
fffff803`09cd0000 fffff803`09cdb000 msisadrv (deferred)
fffff803`09ce0000 fffff803`09d57000 pci (deferred)
fffff803`09d60000 fffff803`09d75000 vdrvroot (deferred)
fffff803`09d80000 fffff803`09db0000 pdc (deferred)
0: kd>
Type here to search
31°C 多雲
1:59 PM
7/14/2025

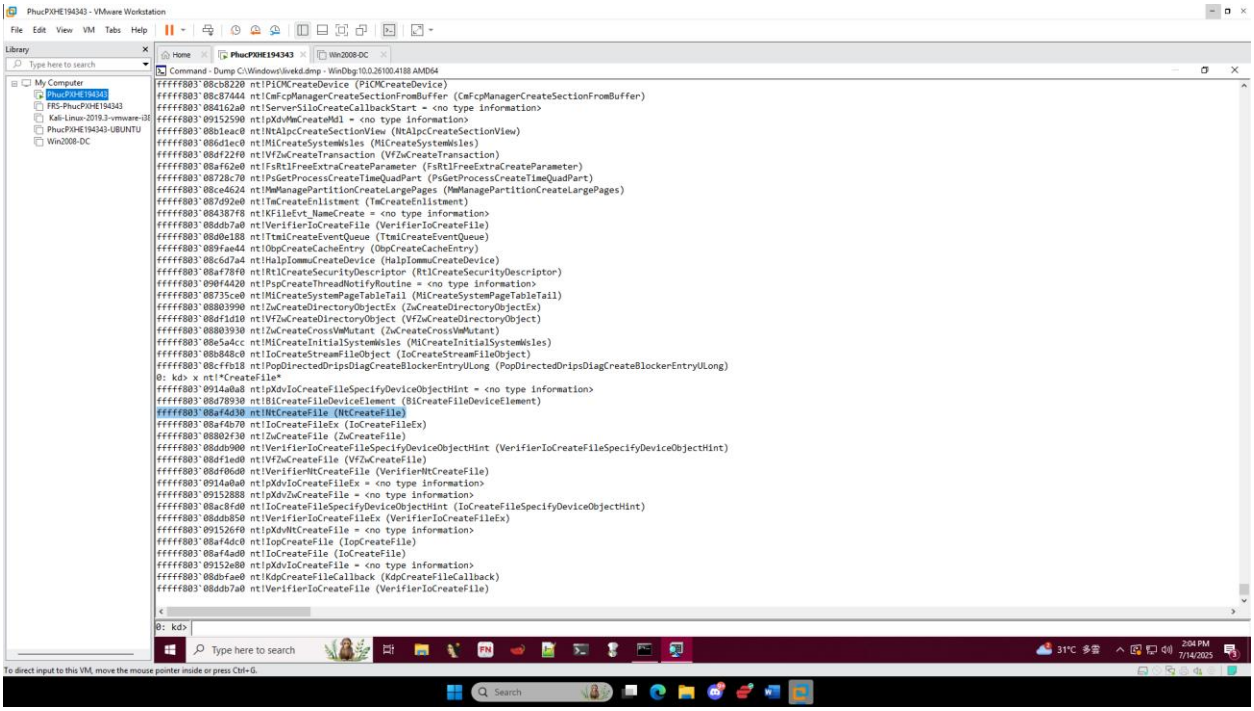

PhucPXHE194343 - VMware Workstation
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
For analysis of this file, run !analyze -v
Unable to load image \??\C:\Windows\system32\Drivers\LiveKdD.SYS, Win32 error 0n2
0: kd> lm
start end module name
fffed91`3d740000 fffed91`3d7db000 win32k (deferred)
fffed91`3d970000 fffed91`3dc47000 win32kbase (deferred)
fffed91`3e1f0000 fffed91`3e5a4000 win32kfull (deferred)
fffed91`3e5b0000 fffed91`3e5f9000 cdd (deferred)
fffff803`07e80000 fffff803`0810f000 mcupdate_GenuineIntel (deferred)
fffff803`08110000 fffff803`08116000 hal (deferred)
fffff803`08120000 fffff803`0812b000 kd (deferred)
fffff803`08130000 fffff803`08158000 tm (deferred)
fffff803`08160000 fffff803`081ce000 CLFS (deferred)
fffff803`081d0000 fffff803`081ea000 PSHED (deferred)
fffff803`081f0000 fffff803`081fb000 BOOTVID (deferred)
fffff803`08200000 fffff803`0826d000 FLTMGR (deferred)
fffff803`08270000 fffff803`0827c000 ntosext (deferred)
fffff803`08408000 fffff803`0944e000 nt (pdb symbols) c:\symbols\ntkrnlmp.pdb\10EFC2288044B448D2954F042A3396E01\ntkrnlmp.pdb
fffff803`09600000 fffff803`09717000 clipsp (deferred)
fffff803`09720000 fffff803`0974c000 ksecdd (deferred)
fffff803`09750000 fffff803`097b2000 msrpc (deferred)
fffff803`097c0000 fffff803`097d0000 cmimcext (deferred)
fffff803`097e0000 fffff803`097f1000 werkernel (deferred)
fffff803`09800000 fffff803`098ec000 CI (deferred)
fffff803`098f0000 fffff803`099ab000 cng (deferred)
fffff803`099b0000 fffff803`099c3000 WDFLDR (deferred)
fffff803`099d0000 fffff803`099df000 SleepStudyHelper (deferred)
fffff803`099e0000 fffff803`099f1000 WppRecorder (deferred)
fffff803`09a00000 fffff803`09ad1000 Wdf01000 (deferred)
fffff803`09ae0000 fffff803`09b06000 acpiex (deferred)
fffff803`09b10000 fffff803`09b1e000 msseccore (deferred)
fffff803`09b20000 fffff803`09bec000 ACPI (deferred)
fffff803`09bf0000 fffff803`09bfc000 WMILIB (deferred)
fffff803`09c00000 fffff803`09c6b000 intelpep (deferred)
fffff803`09c70000 fffff803`09c88000 WindowsTrustedRT (deferred)
fffff803`09c90000 fffff803`09c9b000 IntelTA (deferred)
fffff803`09ca0000 fffff803`09cab000 WindowsTrustedRTProxy (deferred)
fffff803`09cb0000 fffff803`09cc4000 pcw (deferred)
fffff803`09cd0000 fffff803`09cdb000 msisadrv (deferred)
fffff803`09ce0000 fffff803`09d57000 pci (deferred)
fffff803`09d60000 fffff803`09d75000 vdrvroot (deferred)
fffff803`09d80000 fffff803`09db0000 pdc (deferred)
fffff803`09dc0000 fffff803`09dd9000 CEA (deferred)
fffff803`09de0000 fffff803`09e11000 partmgr (deferred)
fffff803`09e20000 fffff803`09ecb000 spaceport (deferred)
0: kd>
Type here to search
31°C 多雲
1:59 PM
7/14/2025

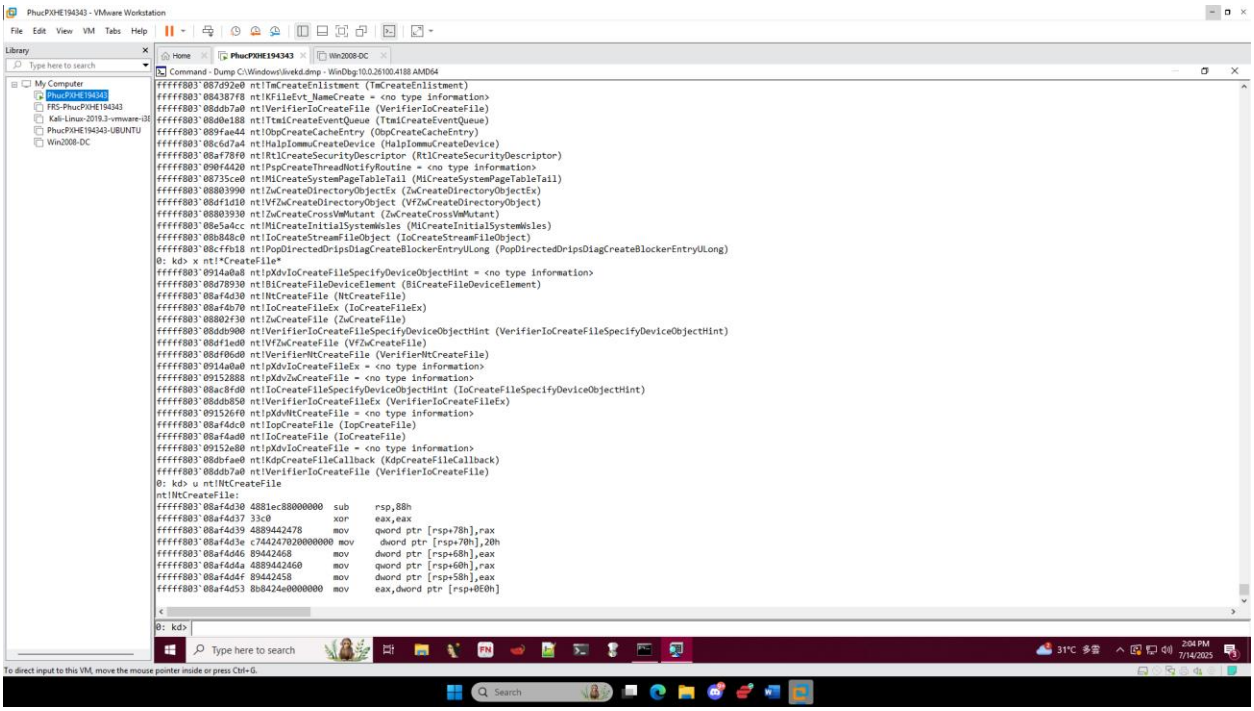

PhucPXHE194343 - VMware Workstation
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
fffff803`10020000 fffff803`100bd000 USBXHCI (deferred)
fffff803`100c0000 fffff803`10104000 ucx01000 (deferred)
fffff803`10110000 fffff803`1011b000 vmgencounter (deferred)
fffff803`10120000 fffff803`1012f000 CmBatt (deferred)
fffff803`10130000 fffff803`10140000 BATTC (deferred)
fffff803`10150000 fffff803`10191000 intelppm (deferred)
fffff803`101a0000 fffff803`101ad000 NdisVirtualBus (deferred)
fffff803`101b0000 fffff803`101bc000 swenum (deferred)
fffff803`101c0000 fffff803`101ce000 rdpbus (deferred)
fffff803`1de00000 fffff803`1de46000 mrxsmb20 (deferred)
fffff803`1de50000 fffff803`1de5a000 vmmemctl (deferred)
fffff803`1de60000 fffff803`1deb6000 srvnet (deferred)
fffff803`1dec0000 fffff803`1ded4000 mmcss (deferred)
fffff803`1dee0000 fffff803`1df07000 Ndu (deferred)
fffff803`1df10000 fffff803`1dfe6000 peauth (deferred)
fffff803`1dff0000 fffff803`1e005000 tcpipreg (deferred)
fffff803`1e010000 fffff803`1e0d7000 srv2 (deferred)
fffff803`1e0e0000 fffff803`1e0fd000 rassstp (deferred)
fffff803`1e100000 fffff803`1e11d000 NDProxy (deferred)
fffff803`1e120000 fffff803`1e14c000 vmhgfs (deferred)
fffff803`1e150000 fffff803`1e162000 condrv (deferred)
fffff803`1e170000 fffff803`1e17e000 wimmount (deferred)
fffff803`1e180000 fffff803`1e18d000 LiveKdD (no symbols)
fffff803`1e580000 fffff803`1e709000 HTTP (deferred)
fffff803`1e710000 fffff803`1e735000 bowser (deferred)
fffff803`1e740000 fffff803`1e75a000 mpsdrv (deferred)
fffff803`1e760000 fffff803`1e7f4000 mrxsmb (deferred)
Unloaded modules:
fffff803`0b4d0000 fffff803`0b4e0000 dump_storport.sys
fffff803`0b510000 fffff803`0b540000 dump_stornvme.sys
fffff803`0b560000 fffff803`0b57e000 dump_dumpfve.sys
fffff803`0cad0000 fffff803`0caed000 dam.sys
fffff803`0acf0000 fffff803`0ad01000 hwpolicy.sys
0: kd> dd nt
fffff803`08408000 00905a4d 00000003 00000004 0000ffff
fffff803`08408010 000000b8 00000000 00000040 00000000
fffff803`08408020 00000000 00000000 00000000 00000000
fffff803`08408030 00000000 00000000 00000000 00000118
fffff803`08408040 0eba1f0e cd09b400 4c01b821 685421cd
fffff803`08408050 70207369 72676f72 63206d61 6f6e6e61
fffff803`08408060 65622074 6e757220 206e6920 20534f44
fffff803`08408070 65646f6d 0a0d0d2e 00000024 00000000
0: kd> da nt
fffff803`08408000 "MZ."
0: kd>
Type here to search
31°C 多雲
2:01 PM
7/14/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search

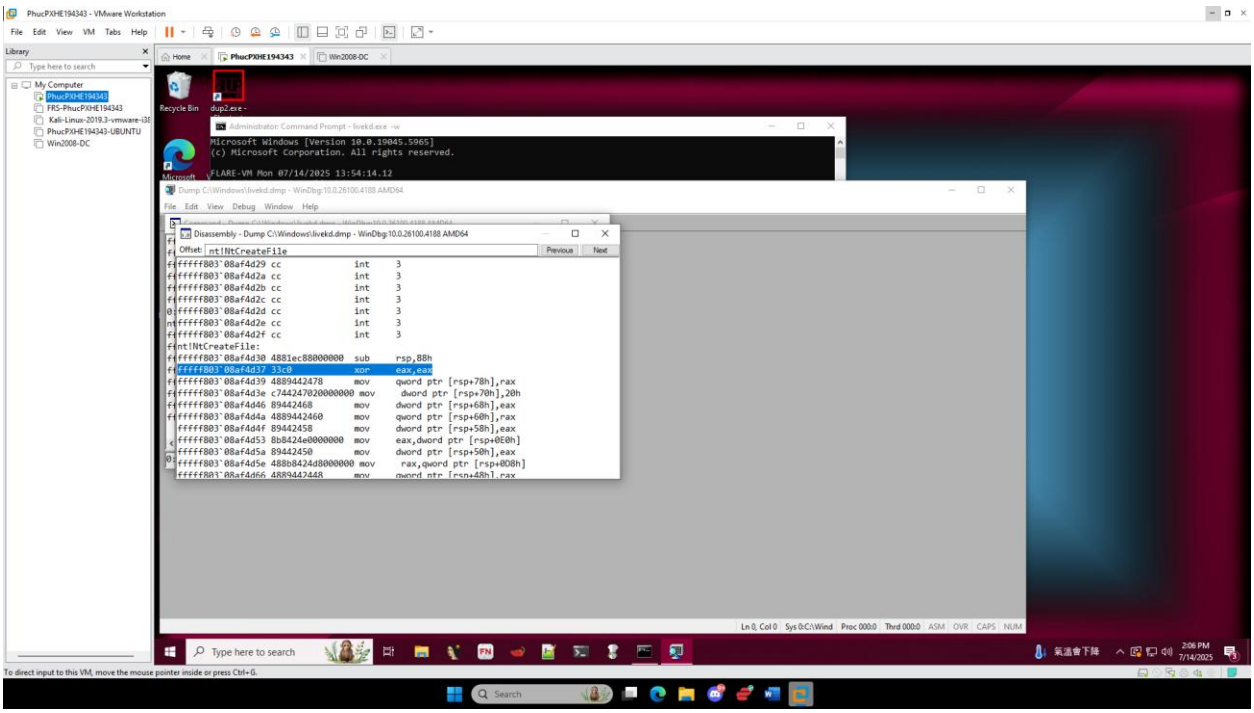

PhucPXHE194343 - VMware Workstation
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
fffff803`10120000 fffff803`1012f000 CmBatt (deferred)
fffff803`10130000 fffff803`10140000 BATTC (deferred)
fffff803`10150000 fffff803`10191000 intelppm (deferred)
fffff803`101a0000 fffff803`101ad000 NdisVirtualBus (deferred)
fffff803`101b0000 fffff803`101bc000 swenum (deferred)
fffff803`101c0000 fffff803`101ce000 rdpbus (deferred)
fffff803`1de00000 fffff803`1de46000 mrxsmb20 (deferred)
fffff803`1de50000 fffff803`1de5a000 vmmemctl (deferred)
fffff803`1de60000 fffff803`1deb6000 srvnet (deferred)
fffff803`1dec0000 fffff803`1ded4000 mmcss (deferred)
fffff803`1dee0000 fffff803`1df07000 Ndu (deferred)
fffff803`1df10000 fffff803`1dfe6000 peauth (deferred)
fffff803`1dff0000 fffff803`1e005000 tcpipreg (deferred)
fffff803`1e010000 fffff803`1e0d7000 srv2 (deferred)
fffff803`1e0e0000 fffff803`1e0fd000 rassstp (deferred)
fffff803`1e100000 fffff803`1e11d000 NDProxy (deferred)
fffff803`1e120000 fffff803`1e14c000 vmhgfs (deferred)
fffff803`1e150000 fffff803`1e162000 condrv (deferred)
fffff803`1e170000 fffff803`1e17e000 wimmount (deferred)
fffff803`1e180000 fffff803`1e18d000 LiveKdD (no symbols)
fffff803`1e580000 fffff803`1e709000 HTTP (deferred)
fffff803`1e710000 fffff803`1e735000 bowser (deferred)
fffff803`1e740000 fffff803`1e75a000 mpsdrv (deferred)
fffff803`1e760000 fffff803`1e7f4000 mrxsmb (deferred)
Unloaded modules:
fffff803`0b4d0000 fffff803`0b4e0000 dump_storport.sys
fffff803`0b510000 fffff803`0b540000 dump_stornvme.sys
fffff803`0b560000 fffff803`0b57e000 dump_dumpfve.sys
fffff803`0cad0000 fffff803`0caed000 dam.sys
fffff803`0acf0000 fffff803`0ad01000 hwpolicy.sys
0: kd> dd nt
fffff803`08408000 00905a4d 00000003 00000004 0000ffff
fffff803`08408010 000000b8 00000000 00000040 00000000
fffff803`08408020 00000000 00000000 00000000 00000000
fffff803`08408030 00000000 00000000 00000000 00000118
fffff803`08408040 0eba1f0e cd09b400 4c01b821 685421cd
fffff803`08408050 70207369 72676f72 63206d61 6f6e6e61
fffff803`08408060 65622074 6e757220 206e6920 20534f44
fffff803`08408070 65646f6d 0a0d0d2e 00000024 00000000
0: kd> da nt
fffff803`08408000 "MZ."
0: kd> da nt+4c
fffff803`0840804c ".!This program cannot be run in "
fffff803`0840806c "DOS mode....$"
0: kd>
Type here to search
31°C 多雲
2:01 PM
7/14/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search

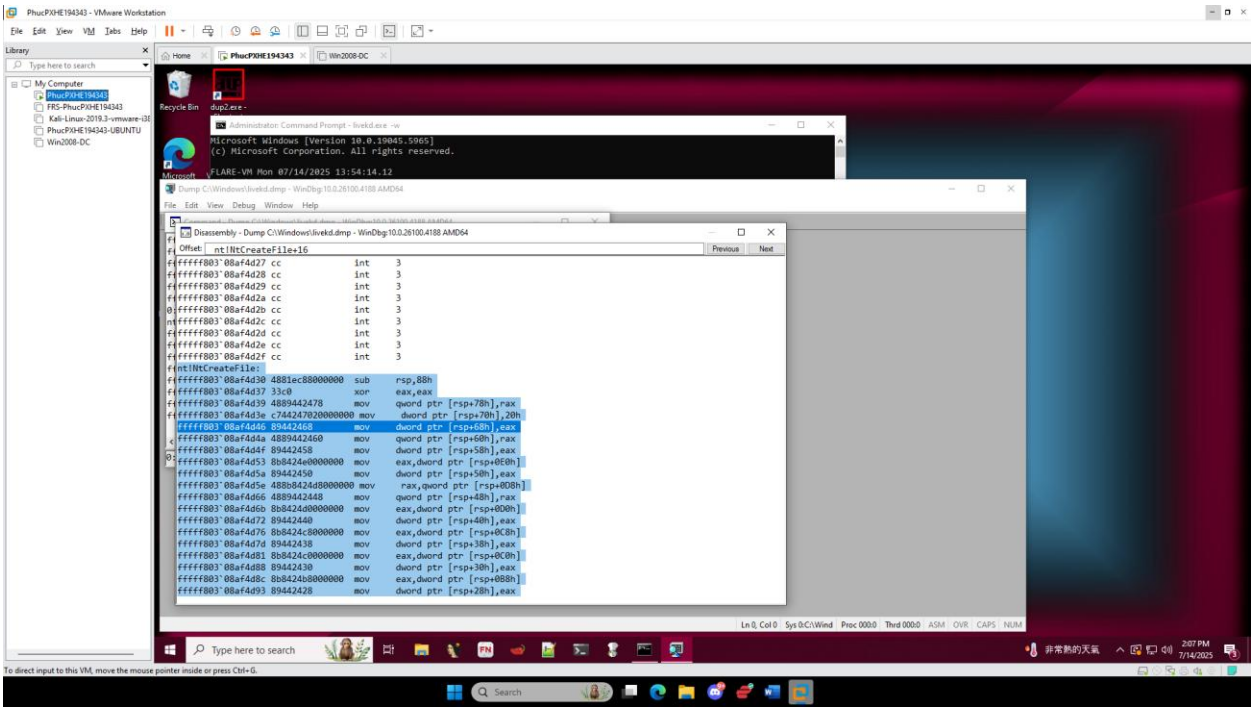

PhucPXHE194343 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
FRS-PhucPXHE194343
Kali-Linux-2019.3-vmware-i38
PhucPXHE194343-UBUNTU
Win2008-DC
Home
PhucPXHE194343
Win2008-DC
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
fffff803`08e513c4 nt!MiFindLargestLoaderDescriptor (MiFindLargestLoaderDescriptor)
fffff803`08be9450 nt! ?? ::NNGAKEGL::`string' (?? ?? ::NNGAKEGL::`string')
fffff803`08bd92c4 nt!RtlpOpenBaseImageFileOptionsKeyEx (RtlpOpenBaseImageFileOptionsKeyEx)
fffff803`091526e8 nt!pXdvKeRestoreExtendedProcessorState = <no type information>
fffff803`08ab7668 nt!AlpcpReturnMessageOnInsufficientBuffer (AlpcpReturnMessageOnInsufficientBuffer)
fffff803`091370a8 nt!CmRegistryMachineSystemCurrentControlSetEnumName = <no type information>
fffff803`084126c8 nt!unconfiguredConfigFlags = <no type information>
fffff803`0901e020 nt!ExCrossVmMutantObjectType = <no type information>
fffff803`09053db4 nt!HalpDmaHibernateRegisterSetIndex = <no type information>
fffff803`084149e0 nt!DEVPKEY_DeviceContainer_IsConnected = <no type information>
fffff803`08bc7e44 nt!IopLogAuditIoRegisterNotificationEvent (IopLogAuditIoRegisterNotificationEvent)
fffff803`089776ac nt!PopCoalescingCheck (PopCoalescingCheck)
fffff803`089303a0 nt!KseDsHookExFreePool (KseDsHookExFreePool)
fffff803`087024d8 nt!MiLockStealSystemVm (MiLockStealSystemVm)
fffff803`08e5651c nt!BapdpRecordIumStatus (BapdpRecordIumStatus)
fffff803`08df3ef0 nt!VfZwQueryFullAttributesFile (VfZwQueryFullAttributesFile)
fffff803`0890e660 nt!IoRaiseInformationalHardError (IoRaiseInformationalHardError)
fffff803`08437568 nt!POP_ETW_EVENT_COMPONENT_IDLE_CONSTRAINTS = <no type information>
fffff803`08bde8c0 nt! ?? ::NNGAKEGL::`string' (?? ?? ::NNGAKEGL::`string')
fffff803`09137290 nt!SepAtomSd = <no type information>
fffff803`08794b84 nt!IopUnmaskInterrupt (IopUnmaskInterrupt)
fffff803`089ab0a0 nt!ViRaiseIrqlToDpcLevel (ViRaiseIrqlToDpcLevel)
fffff803`087fc8a4 nt!MiGetProtectionFromPte (MiGetProtectionFromPte)
fffff803`08539658 nt!_IMPORT_DESCRIPTOR_PSHED = <no type information>
fffff803`08412308 nt!DEVPKEY_Device_DriverDesc = <no type information>
fffff803`0890d770 nt!KeCapturePersistentThreadState (KeCapturePersistentThreadState)
fffff803`090212c0 nt!ExExternalBootSupportInitializationEvent = <no type information>
fffff803`08be4410 nt! ?? ::NNGAKEGL::`string' (?? ?? ::NNGAKEGL::`string')
fffff803`08be3aa0 nt! ?? ::NNGAKEGL::`string' (?? ?? ::NNGAKEGL::`string')
fffff803`08b8e6b0 nt!BiReleasePrivilege (BiReleasePrivilege)
fffff803`09053dd0 nt!HalpDmaPdoListLock = <no type information>
fffff803`08c6fd00 nt!HalpLbrStopRecording (HalpLbrStopRecording)
fffff803`08ce57e0 nt!ObOpenObjectByPointerWithTag (ObOpenObjectByPointerWithTag)
fffff803`0881d150 nt! ?? ::FNODOBFM::`string' (?? ?? ::FNODOBFM::`string')
fffff803`087bf08c nt!RtlApplyImportRelocationToImage (RtlApplyImportRelocationToImage)
fffff803`088c4510 nt!HalEnumerateEnvironmentVariablesEx (HalEnumerateEnvironmentVariablesEx)
fffff803`08ea09c8 nt! ?? ::EKOMKFNL::`string' = <no type information>
fffff803`08a2b610 nt!CcPinRead (CcPinRead)
fffff803`08ea1ea8 nt!CmpFlagsString = <no type information>
fffff803`0904cab0 nt!IopNumberDeviceNodes = <no type information>
fffff803`088ff940 nt!Hv1SvmSetDeviceEnabled (Hv1SvmSetDeviceEnabled)
fffff803`087da4c nt!CmDeleteCommonClassRegKey (_CmDeleteCommonClassRegKey)
fffff803`08bde830 nt! ?? ::NNGAKEGL::`string' (?? ?? ::NNGAKEGL::`string')
fffff803`08deb190 nt!VerifierExEnterPriorityRegionAndAcquireResourceShared (VerifierExEnterPriorityRegionAndAcquireResourceShared)
0: kd>
Type here to search
31°C 多雲
2:02 PM
7/14/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search


PhucPXHE194343 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
FRS-PhucPXHE194343
Kali-Linux-2019.3-vmware-i38
PhucPXHE194343-UBUNTU
Win2008-DC
Home
PhucPXHE194343
Win2008-DC
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
fffff803`08e5a5c0 nt!MiCreateKernelHalSlabRange (MiCreateKernelHalSlabRange)
fffff803`091369dc nt!PspCreateProcessNotifyRoutineCount = <no type information>
fffff803`087fe734 nt!MiCreateInitialLargeLeafPfns (MiCreateInitialLargeLeafPfns)
fffff803`08aaa4d8 nt!MiValidateSectionCreate (MiValidateSectionCreate)
fffff803`09051d28 nt!HalpIommuDeviceCreatedListPushLock = <no type information>
fffff803`08de1f94 nt!ViThunkCreateThunkTable (ViThunkCreateThunkTable)
fffff803`08987df0 nt!PopSqmCreateDwordStreamEntry (PopSqmCreateDwordStreamEntry)
fffff803`08df2260 nt!VfZwCreateTimer (VfZwCreateTimer)
fffff803`08d89220 nt!ObCreateSiloRootDirectory (ObCreateSiloRootDirectory)
fffff803`09152898 nt!pXdvZwCreateDirectoryObject = <no type information>
fffff803`08a85ce4 nt!PopStatsCreatePowerRequest (PopStatsCreatePowerRequest)
fffff803`087d8e60 nt!NtCreateEnlistment (NtCreateEnlistment)
fffff803`08c80720 nt!CmpCreateHwProfileFriendlyName (CmpCreateHwProfileFriendlyName)
fffff803`08b88d80 nt!IoCreateArcName (IoCreateArcName)
fffff803`08b7027c nt!PiDqObjectActionQueueEntryCreate (PiDqObjectActionQueueEntryCreate)
fffff803`08539610 nt!_imp_MesDecodeBufferHandleCreate = <no type information>
fffff803`08803b90 nt!ZwCreatePort (ZwCreatePort)
fffff803`08af3ad0 nt!NtCreateUserProcess (NtCreateUserProcess)
fffff803`08ddae80 nt!VerifierExUuidCreate (VerifierExUuidCreate)
fffff803`08d7d830 nt!CmCreateInstallerClass (_CmCreateInstallerClass)
fffff803`089fb390 nt!RtlCreateAcl (RtlCreateAcl)
fffff803`08d2bb80 nt!SepCreateSidValuesBlock (SepCreateSidValuesBlock)
fffff803`08cd0d44 nt!MiLogCreateImageFileMapFailure (MiLogCreateImageFileMapFailure)
fffff803`08a31f30 nt!ExpNodeCreateSystemThread (ExpNodeCreateSystemThread)
fffff803`08bd4420 nt!FsRtlInitExtraCreateParameterLookasideList (FsRtlInitExtraCreateParameterLookasideList)
fffff803`088c28ec nt!HalpCreateMcaProcessorErrorRecord (HalpCreateMcaProcessorErrorRecord)
fffff803`091528c0 nt!pXdvZwCreateSection = <no type information>
fffff803`08a21430 nt!FsRtlFindExtraCreateParameter (FsRtlFindExtraCreateParameter)
fffff803`08d0d44c nt!TtmiLogTerminalCreated (TtmiLogTerminalCreated)
fffff803`08b96f90 nt!NtCreateWaitablePort (NtCreateWaitablePort)
fffff803`09152b90 nt!pXdvZwAlpcCreatePort = <no type information>
fffff803`08930c0c nt!KsepDsEventIoCreateDevice (KsepDsEventIoCreateDevice)
fffff803`08a214c0 nt!FsRtlRemoveExtraCreateParameter (FsRtlRemoveExtraCreateParameter)
fffff803`08afe460 nt!MmCreateSectionEx (MmCreateSectionEx)
fffff803`08c96d00 nt!SC_ENV::CreateGuid (public: static long __cdecl SC_ENV::CreateGuid(struct _GUID *))
fffff803`08802d90 nt!ZwCreateEvent (ZwCreateEvent)
fffff803`087c7038 nt!PopFxCreateDeviceCommon (PopFxCreateDeviceCommon)
fffff803`08b98980 nt!RtlpMuiRegCreateLanguages (RtlpMuiRegCreateLanguages)
fffff803`087d8e80 nt!NtCreateResourceManager (NtCreateResourceManager)
fffff803`09152ad8 nt!pXdvZwCreateTransaction = <no type information>
fffff803`08b3fd10 nt!PiSwDeviceCreate (PiSwDeviceCreate)
fffff803`08962610 nt!MiCreateCloneChain (MiCreateCloneChain)
fffff803`08df03a0 nt!VerifierNtCreateSection (VerifierNtCreateSection)
fffff803`09152ec0 nt!pXdvIoCreateUnprotectedSymbolicLink = <no type information>
fffff803`088c24d0 nt!HalpCreateErrorRecord (HalpCreateErrorRecord)
0: kd> x nt!*CreateFile*
Type here to search
31°C 多雲
2:03 PM
7/14/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search


PhucPXHE194343 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
FRS-PhucPXHE194343
Kali-Linux-2019.3-vmware-i38
PhucPXHE194343-UBUNTU
Win2008-DC
Home
PhucPXHE194343
Win2008-DC
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
fffff803`08cb8220 nt!PiCMCreateDevice (PiCMCreateDevice)
fffff803`08c87444 nt!CmFcpManagerCreateSectionFromBuffer (CmFcpManagerCreateSectionFromBuffer)
fffff803`084162a0 nt!ServerSiloCreateCallbackStart = <no type information>
fffff803`09152590 nt!pXdvMwCreateMdl = <no type information>
fffff803`08b1eac0 nt!NtAlpcCreateSectionView (NtAlpcCreateSectionView)
fffff803`086d1ec0 nt!MiCreateSystemWsles (MiCreateSystemWsles)
fffff803`08df22f0 nt!VfZwCreateTransaction (VfZwCreateTransaction)
fffff803`08af62e0 nt!FsRtlFreeExtraCreateParameter (FsRtlFreeExtraCreateParameter)
fffff803`08728c70 nt!PsGetProcessCreateTimeQuadPart (PsGetProcessCreateTimeQuadPart)
fffff803`08ce4624 nt!MmManagePartitionCreateLargePages (MmManagePartitionCreateLargePages)
fffff803`087d92e0 nt!TmCreateEnlistment (TmCreateEnlistment)
fffff803`084387f8 nt!KFileEvt_NameCreate = <no type information>
fffff803`08ddb7a0 nt!VerifierIoCreateFile (VerifierIoCreateFile)
fffff803`08d0e188 nt!TtmiCreateEventQueue (TtmiCreateEventQueue)
fffff803`089fae44 nt!ObpCreateCacheEntry (ObpCreateCacheEntry)
fffff803`08c6d7a4 nt!HalpIommuCreateDevice (HalpIommuCreateDevice)
fffff803`08af78f0 nt!RtlCreateSecurityDescriptor (RtlCreateSecurityDescriptor)
fffff803`090f4420 nt!PspCreateThreadNotifyRoutine = <no type information>
fffff803`08735ce0 nt!MiCreateSystemPageTableTail (MiCreateSystemPageTableTail)
fffff803`08803990 nt!ZwCreateDirectoryObjectEx (ZwCreateDirectoryObjectEx)
fffff803`08df1d10 nt!VfZwCreateDirectoryObject (VfZwCreateDirectoryObject)
fffff803`08803930 nt!ZwCreateCrossVmMutant (ZwCreateCrossVmMutant)
fffff803`08e5a4cc nt!MiCreateInitialSystemWsles (MiCreateInitialSystemWsles)
fffff803`08b848c0 nt!IoCreateStreamFileObject (IoCreateStreamFileObject)
fffff803`08cffb18 nt!PopDirectedDripsDiagCreateBlockerEntryULong (PopDirectedDripsDiagCreateBlockerEntryULong)
0: kd> x nt!*CreateFile*
fffff803`0914a0a8 nt!pXdvIoCreateFileSpecifyDeviceObjectHint = <no type information>
fffff803`08d78930 nt!BiCreateFileDeviceElement (BiCreateFileDeviceElement)
fffff803`08af4d30 nt!NtCreateFile (NtCreateFile)
fffff803`08af4b70 nt!IoCreateFileEx (IoCreateFileEx)
fffff803`08802f30 nt!ZwCreateFile (ZwCreateFile)
fffff803`08ddb900 nt!VerifierIoCreateFileSpecifyDeviceObjectHint (VerifierIoCreateFileSpecifyDeviceObjectHint)
fffff803`08df1ed0 nt!VfZwCreateFile (VfZwCreateFile)
fffff803`08df06d0 nt!VerifierNtCreateFile (VerifierNtCreateFile)
fffff803`0914a0a0 nt!pXdvIoCreateFileEx = <no type information>
fffff803`09152888 nt!pXdvZwCreateFile = <no type information>
fffff803`08ac8fd0 nt!IoCreateFileSpecifyDeviceObjectHint (IoCreateFileSpecifyDeviceObjectHint)
fffff803`08ddb850 nt!VerifierIoCreateFileEx (VerifierIoCreateFileEx)
fffff803`091526f0 nt!pXdvNtCreateFile = <no type information>
fffff803`08af4dc0 nt!IopCreateFile (IopCreateFile)
fffff803`08af4ad0 nt!IoCreateFile (IoCreateFile)
fffff803`09152e80 nt!pXdvIoCreateFile = <no type information>
fffff803`08dbfae0 nt!KdpCreateFileCallback (KdpCreateFileCallback)
fffff803`08ddb7a0 nt!VerifierIoCreateFile (VerifierIoCreateFile)
0: kd>
Type here to search
31°C 多雲
2:04 PM
7/14/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search


PhucPXHE194343 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
PhucPXHE194343
FRS-PhucPXHE194343
Kali-Linux-2019.3-vmware-i38
PhucPXHE194343-UBUNTU
Win2008-DC
Home
PhucPXHE194343
Win2008-DC
Command - Dump C:\Windows\livekd.dmp - WinDbg:10.0.26100.4188 AMD64
fffff803`087d92e0 nt!TmCreateEnlistment (TmCreateEnlistment)
fffff803`084387f8 nt!KFileEvt_NameCreate = <no type information>
fffff803`08ddb7a0 nt!VerifierIoCreateFile (VerifierIoCreateFile)
fffff803`08d0e188 nt!TtmiCreateEventQueue (TtmiCreateEventQueue)
fffff803`089fae44 nt!ObpCreateCacheEntry (ObpCreateCacheEntry)
fffff803`08c6d7a4 nt!HalpIommuCreateDevice (HalpIommuCreateDevice)
fffff803`08af78f0 nt!RtlCreateSecurityDescriptor (RtlCreateSecurityDescriptor)
fffff803`090f4420 nt!PspCreateThreadNotifyRoutine = <no type information>
fffff803`08735ce0 nt!MiCreateSystemPageTableTail (MiCreateSystemPageTableTail)
fffff803`08803990 nt!ZwCreateDirectoryObjectEx (ZwCreateDirectoryObjectEx)
fffff803`08df1d10 nt!VfZwCreateDirectoryObject (VfZwCreateDirectoryObject)
fffff803`08803930 nt!ZwCreateCrossVmMutant (ZwCreateCrossVmMutant)
fffff803`08e5a4cc nt!MiCreateInitialSystemWsles (MiCreateInitialSystemWsles)
fffff803`08b848c0 nt!IoCreateStreamFileObject (IoCreateStreamFileObject)
fffff803`08cffb18 nt!PopDirectedDripsDiagCreateBlockerEntryULong (PopDirectedDripsDiagCreateBlockerEntryULong)
0: kd> x nt!*CreateFile*
fffff803`0914a0a8 nt!pXdvIoCreateFileSpecifyDeviceObjectHint = <no type information>
fffff803`08d78930 nt!BiCreateFileDeviceElement (BiCreateFileDeviceElement)
fffff803`08af4d30 nt!NtCreateFile (NtCreateFile)
fffff803`08af4b70 nt!IoCreateFileEx (IoCreateFileEx)
fffff803`08802f30 nt!ZwCreateFile (ZwCreateFile)
fffff803`08ddb900 nt!VerifierIoCreateFileSpecifyDeviceObjectHint (VerifierIoCreateFileSpecifyDeviceObjectHint)
fffff803`08df1ed0 nt!VfZwCreateFile (VfZwCreateFile)
fffff803`08df06d0 nt!VerifierNtCreateFile (VerifierNtCreateFile)
fffff803`0914a0a0 nt!pXdvIoCreateFileEx = <no type information>
fffff803`09152888 nt!pXdvZwCreateFile = <no type information>
fffff803`08ac8fd0 nt!IoCreateFileSpecifyDeviceObjectHint (IoCreateFileSpecifyDeviceObjectHint)
fffff803`08ddb850 nt!VerifierIoCreateFileEx (VerifierIoCreateFileEx)
fffff803`091526f0 nt!pXdvNtCreateFile = <no type information>
fffff803`08af4dc0 nt!IopCreateFile (IopCreateFile)
fffff803`08af4ad0 nt!IoCreateFile (IoCreateFile)
fffff803`09152e80 nt!pXdvIoCreateFile = <no type information>
fffff803`08dbfae0 nt!KdpCreateFileCallback (KdpCreateFileCallback)
fffff803`08ddb7a0 nt!VerifierIoCreateFile (VerifierIoCreateFile)
0: kd> u nt!NtCreateFile
nt!NtCreateFile:
fffff803`08af4d30 4881ec88000000 sub   rsp,88h
fffff803`08af4d37 33c0   xor   eax,eax
fffff803`08af4d39 4889442478   mov   qword ptr [rsp+78h],rax
fffff803`08af4d3e c744247020000000 mov   dword ptr [rsp+70h],20h
fffff803`08af4d46 89442468   mov   dword ptr [rsp+68h],eax
fffff803`08af4d4a 4889442460   mov   qword ptr [rsp+60h],rax
fffff803`08af4d4f 89442458   mov   dword ptr [rsp+58h],eax
fffff803`08af4d53 8b8424e0000000 mov   eax,dword ptr [rsp+0E0h]
0: kd>
Type here to search
31°C 多雲
2:04 PM
7/14/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search



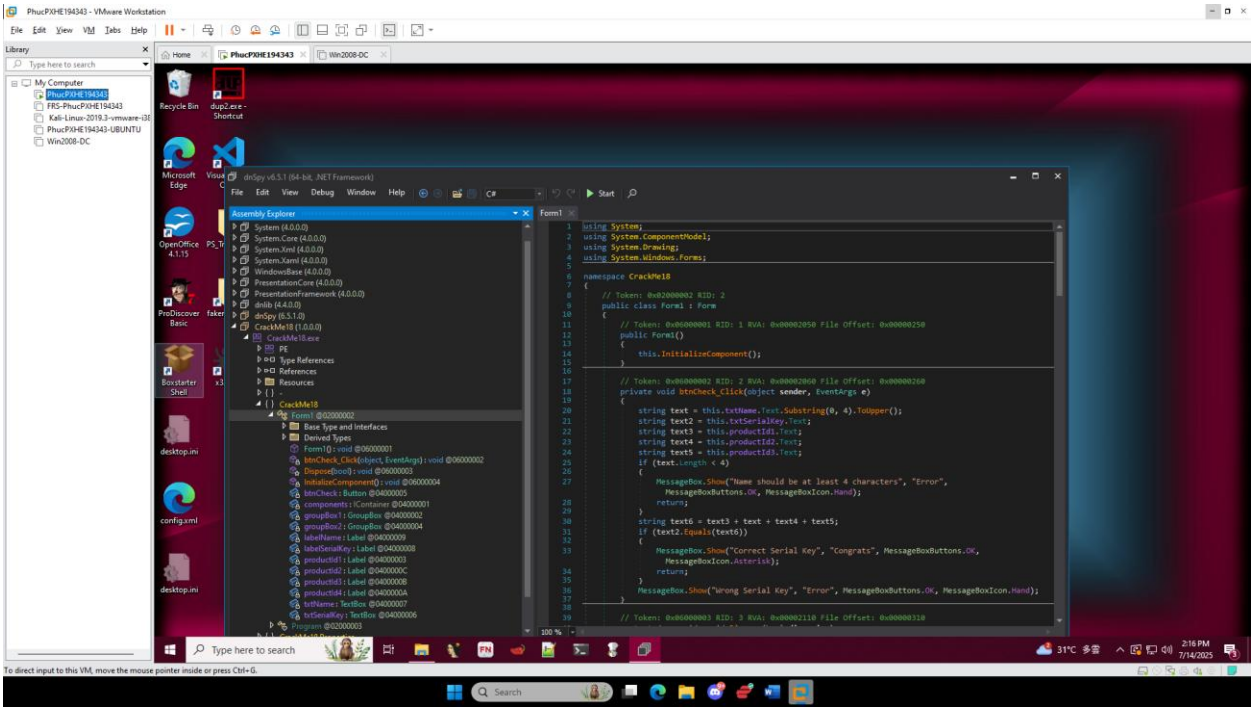


Crack Me 18

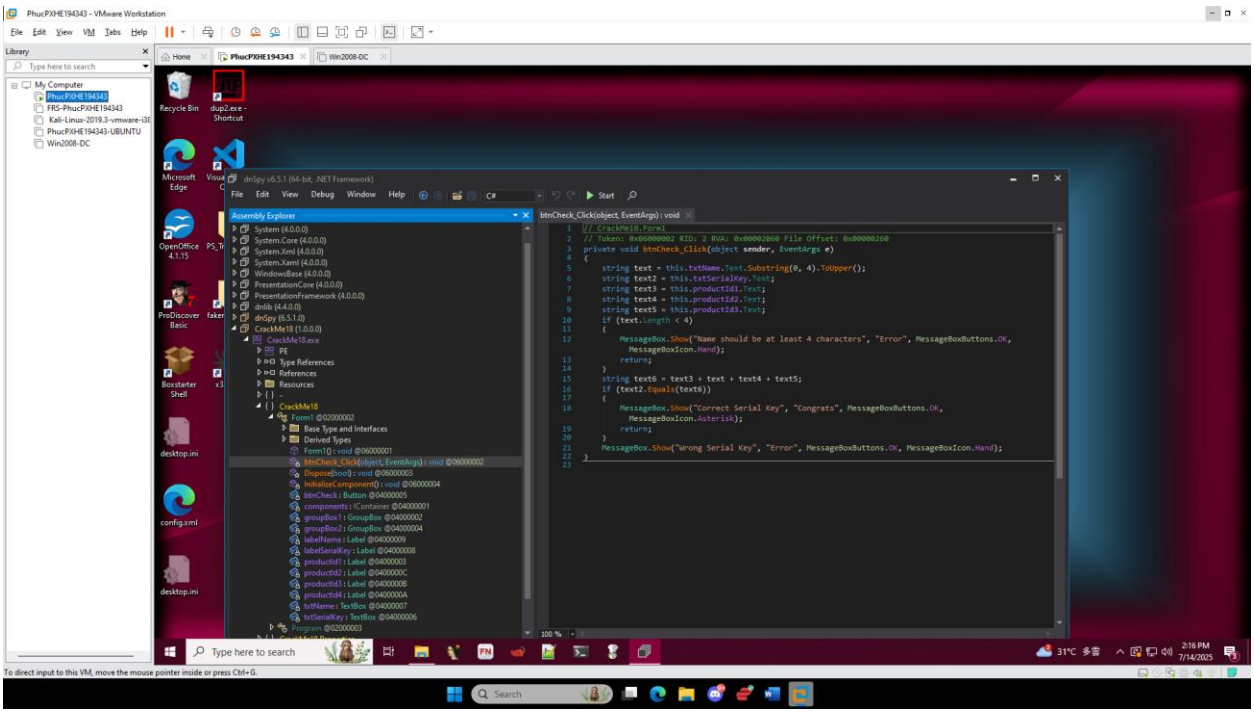
bài này phải chú ý phần viết bằng C# và nó là một .NET framework có thể thực thi được nên em sẽ sử dụng một công cụ có tên dnSpy vì nó có thể decompile C#

Part 1: Patch it to always succeed no matter what name and serial key you enter.

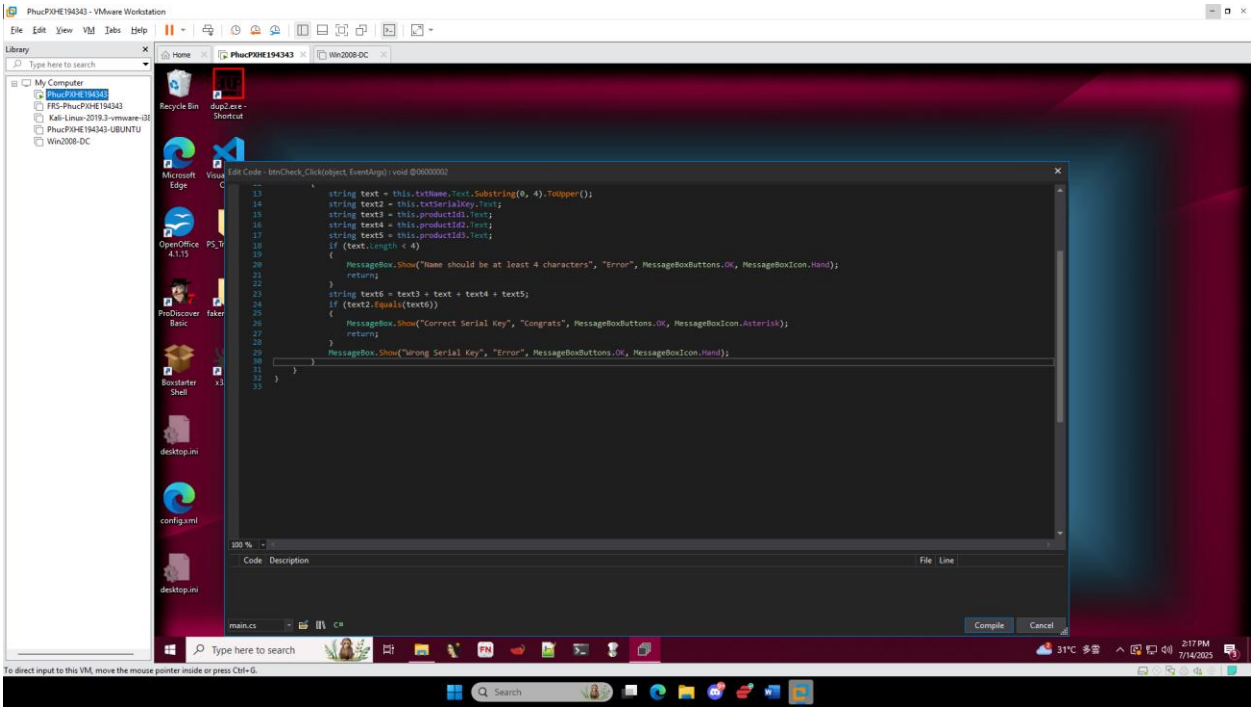
Step 1: Mở dnSpy và mở crackme 18 chúng ta đã thấy được mã nguồn của chương trình



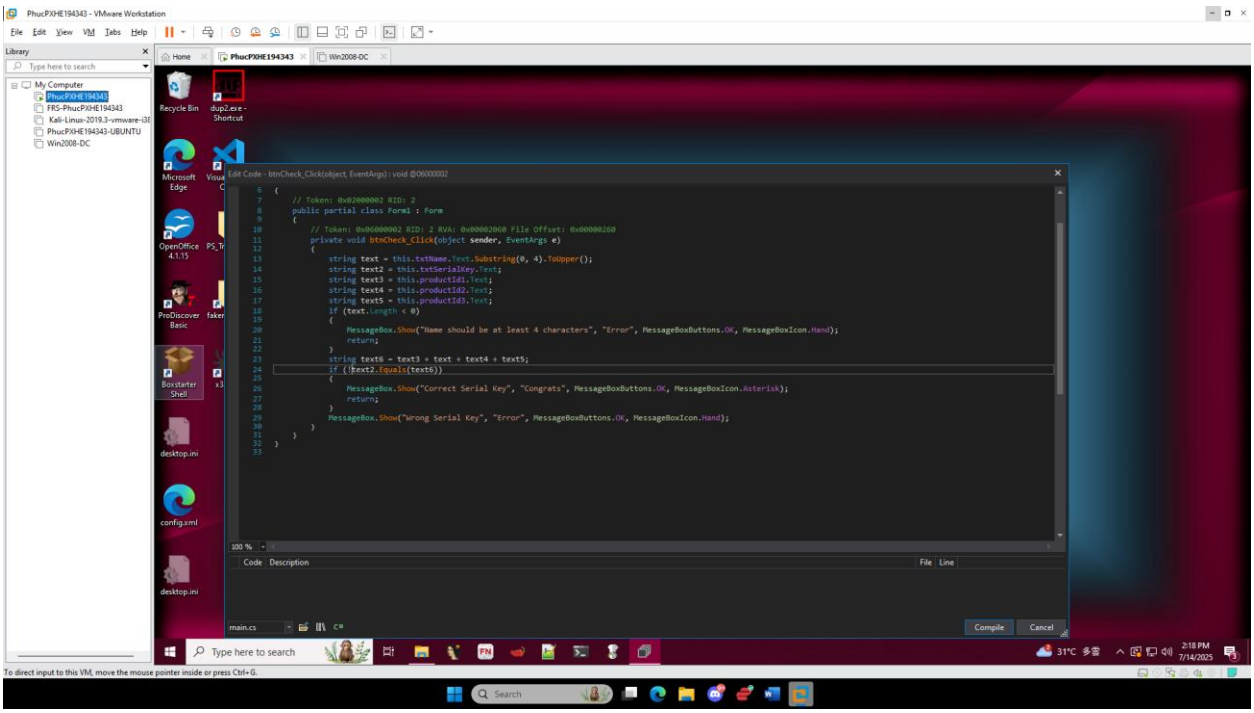
Step 2: Em mở btnCheck_Click, đoạn mã trên khá dễ hiểu: nó gán text và text2 lần lượt là **Name** và **SerialKey**, còn text3, text4, text5 là các **ProductID**. Sau đó, chương trình kiểm tra xem biến text có nhiều hơn 4 ký tự không. Nếu có, nó lấy 4 ký tự đầu tiên của text, chuyển thành chữ in hoa, rồi nối chuỗi lại và so sánh với **SerialKey** mà người dùng đã nhập vào và lưu trong text2.



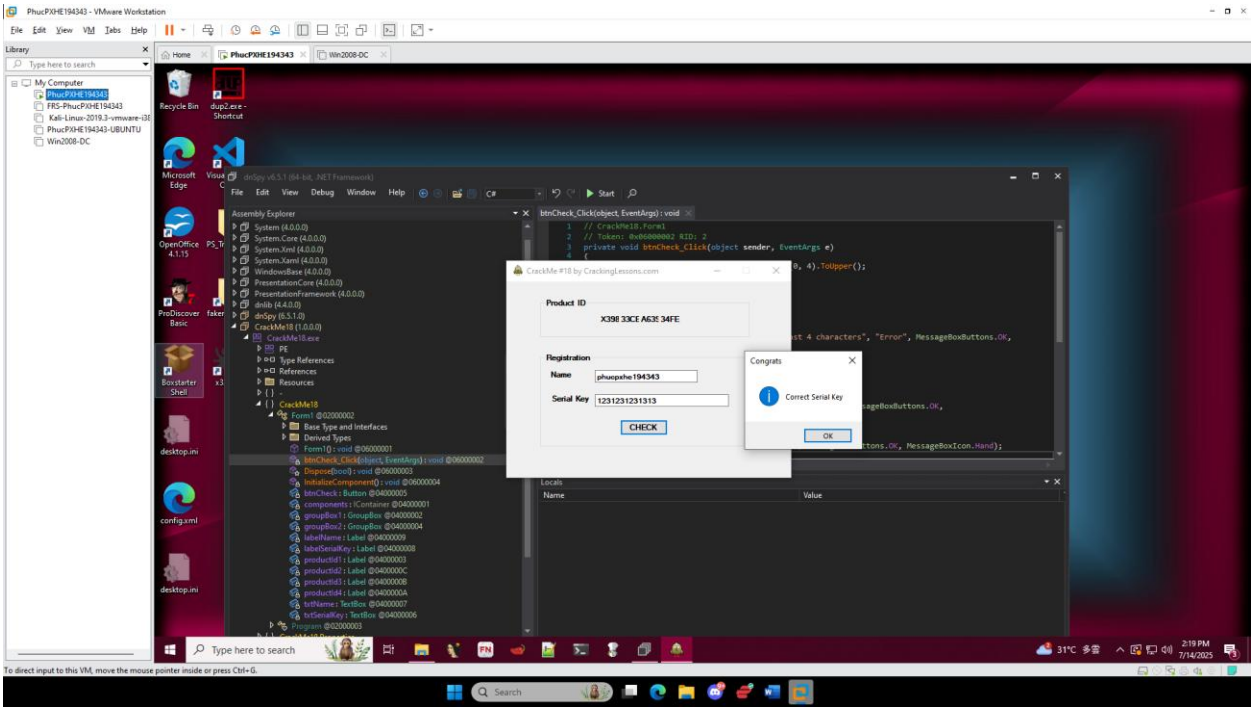
Step 3: Mở edit method lên



Step 4: Sửa dòng 18 và 24 như ảnh để có thể nhập ít hơn 4 kí tự và nhập bất kì cái gì cũng đúng(vì thêm dấu ! là ngược lại)

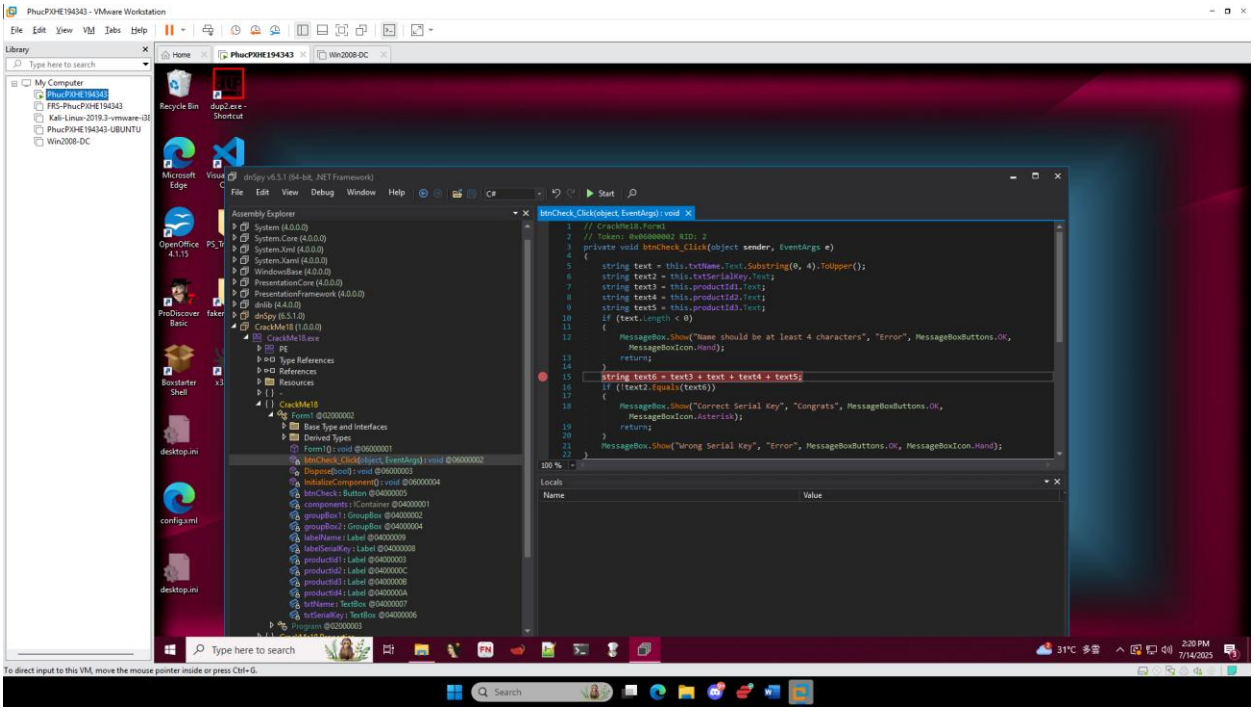


Step 5: Save Module và đã crack Part 1 thành công

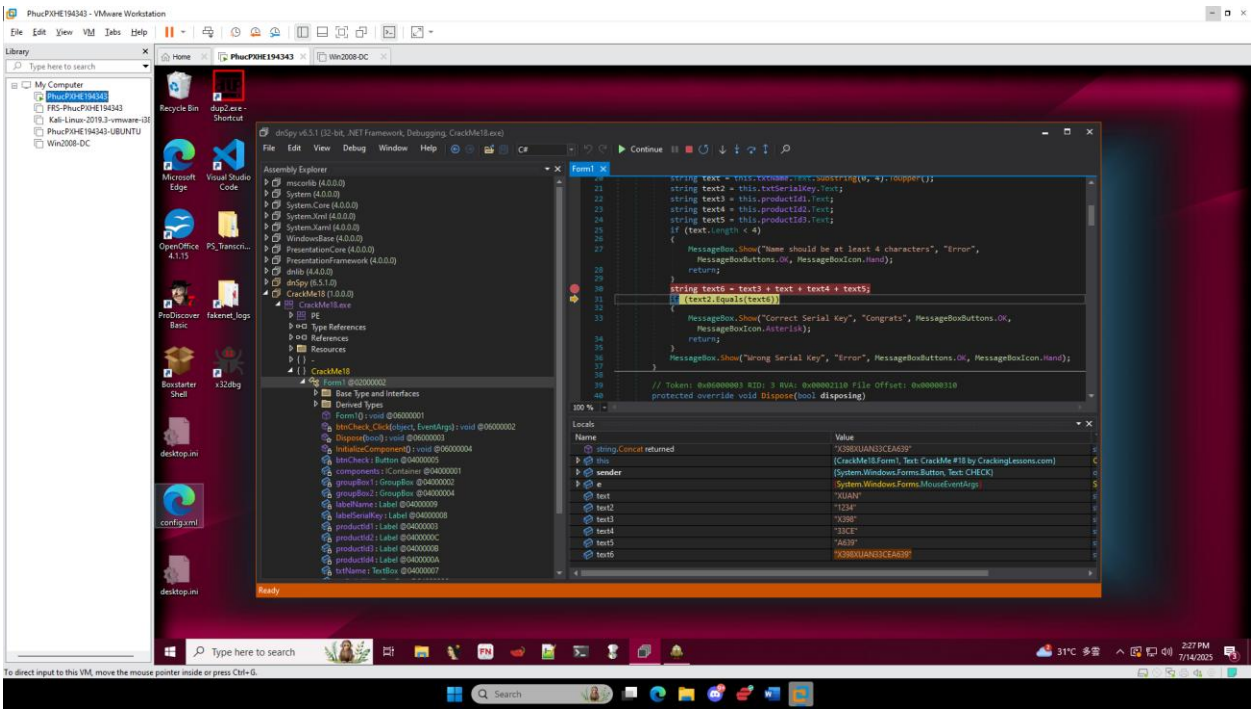


Part 2: Do serial fishing to extract the serial key based on a given name of your choice.

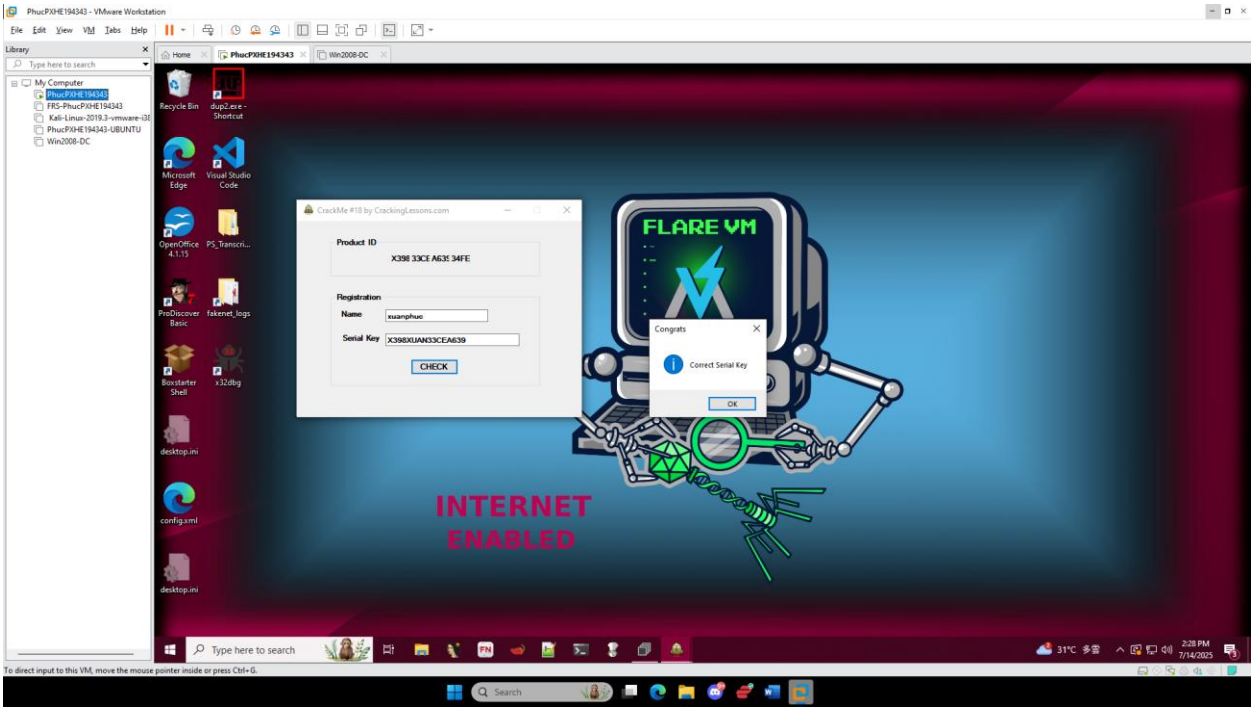
Step 1: Nhiệm vụ tiếp theo của đề bài yêu cầu thực hiện "serial fishing" – tức là trích xuất khóa nối tiếp (Serial Key) dựa trên dữ liệu có sẵn và hành vi của chương trình. Vì vậy, em cho rằng ta cần đặt breakpoint tại vị trí chứa giá trị (value) được dùng để so sánh với SerialKey do người dùng nhập vào. Bởi vì, giá trị này chính là phần mà chương trình sử dụng để xác thực SerialKey, nên việc theo dõi nó sẽ giúp ta tìm ra cách tạo hoặc trích xuất khóa nối tiếp một cách chính xác. Đầu tiền chúng ta sẽ add Breakpoint say đó chạy chương trình



Step 2: Sau khi chương trình dừng tại breakpoint, ta sẽ thực hiện thêm một bước (step over hoặc step into) để quan sát cách giá trị của biến value được lưu hoặc gán như thế nào. Việc này giúp chúng ta hiểu rõ quá trình xử lý chuỗi SerialKey trong bộ nhớ, từ đó hỗ trợ việc phân tích và trích xuất khóa nối tiếp một cách chính xác. Đây chính là key fishing



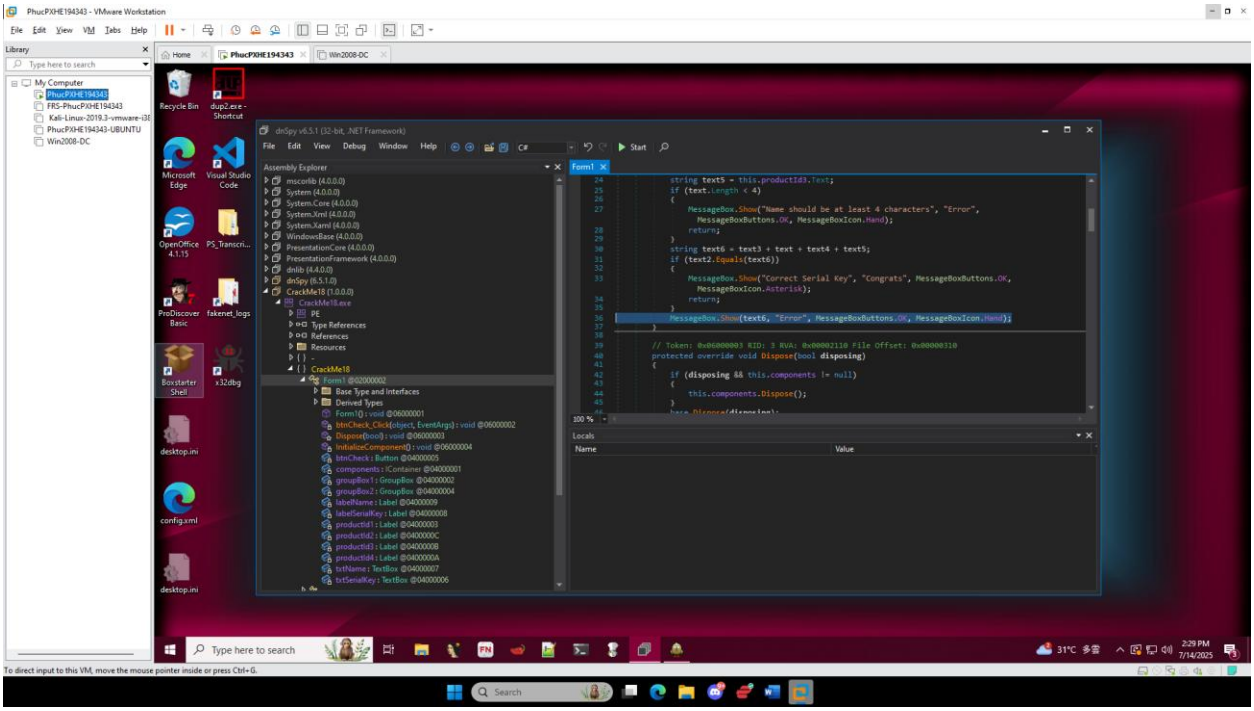
Step 3: Thử key Fishing



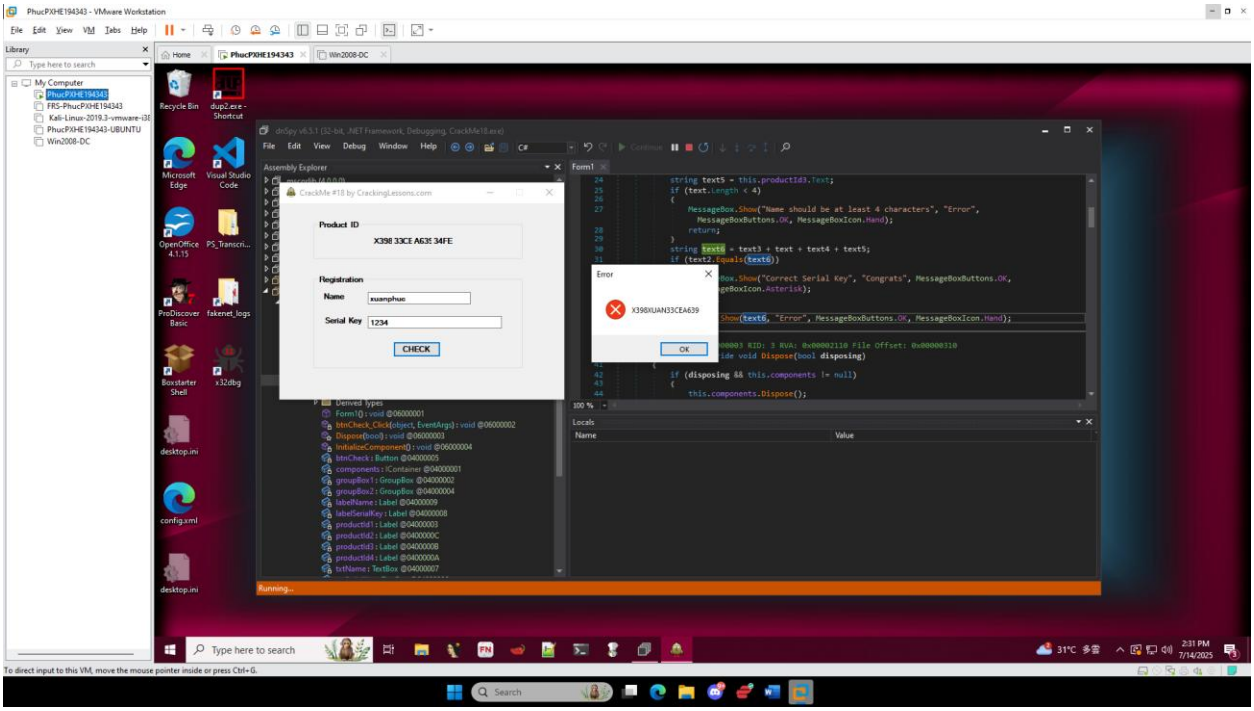
Part 3: Create a keygen

Step: 1

Tương tự như những bài trước, thay vì để chương trình hiển thị thông báo lỗi, em sẽ chỉnh sửa dòng hiển thị lỗi để in ra trực tiếp giá trị value của Serial Key. Bằng cách này, ta có thể dễ dàng lấy được khóa nối tiếp mà không cần phải đoán hay brute-force.



Step 2: Nhập serial key bất kì thì lúc đấy key fishing sẽ được hiển thị


PhucPXHE194343 - VMware Workstation
Product ID
X398 33CE A63E 34FE
Registration
Name
xuanphuc
Serial Key
1234
CHECK
Error
X398XUAN33CEA639
OK
Type here to search