PROJ 13: Using Kernel Debugging Commands with WinDbg

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

Nikhil Patel

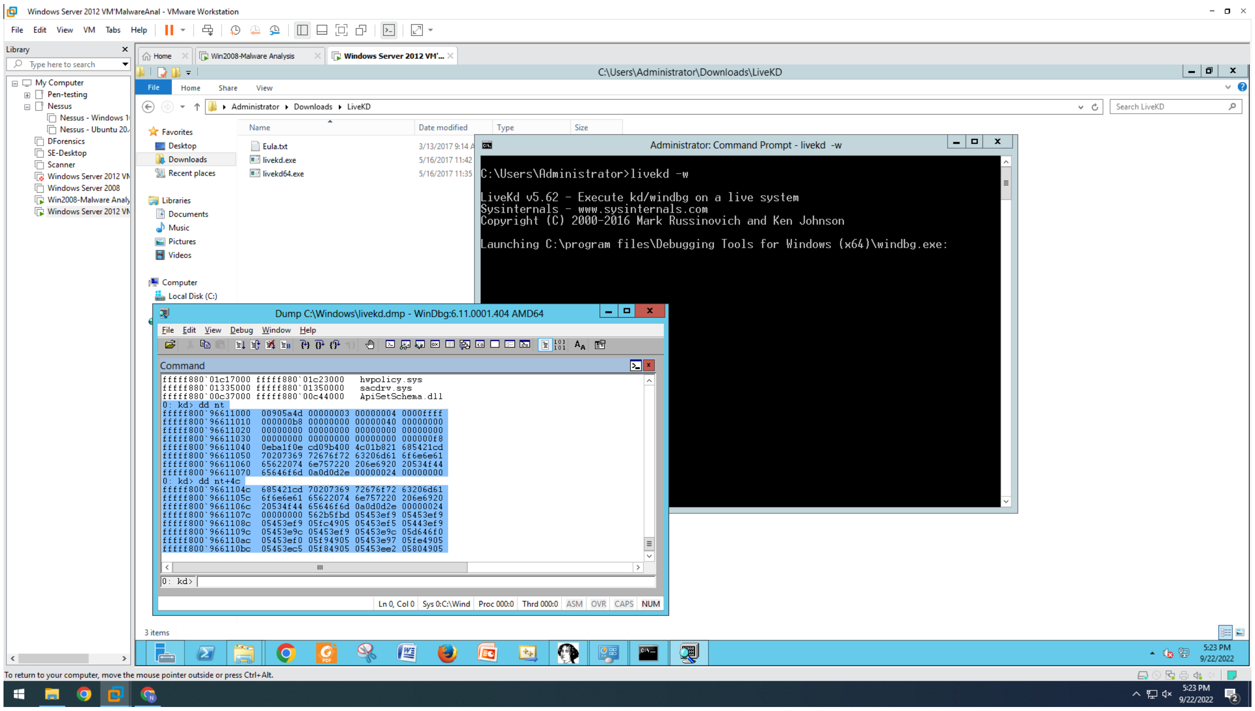
11/09/2022

Introduction: In this lab, we will debug Using Kernel Debugging Commands with WinDbg.

Procedure :

Listing Modules with lm

- Continue lab 12, and type “lm”.

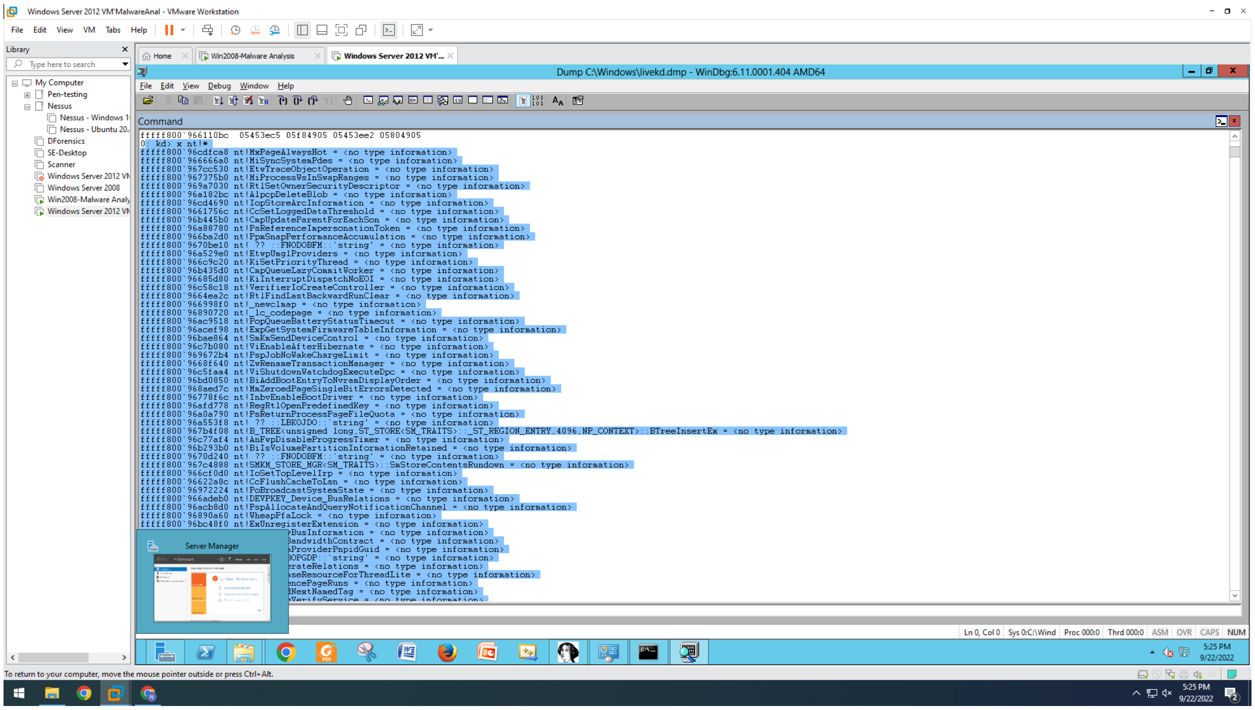


```
C:\Users\Administrator>livekd -w

LiveKd v5.62 - Execute kd/windbg on a live system
Sysinternals - www.sysinternals.com
Copyright (C) 2000-2016 Mark Russinovich and Ken Johnson

Launching C:\program files\Debugging Tools for Windows (x64)\windbg.exe:
```

```
fffff880`01c17000 fffff880`01c23000   hwpolicy.sys
fffff880`01335000 fffff880`01350000   sacdrv.sys
fffff880`00c37000 fffff880`00c44000   ApiSetSchema.dll
0: kd> dd nt
fffff800`96611000  00905a4d 00000003 00000004 0000ffff
fffff800`96611010  000000b8 00000000 00000040 00000000
fffff800`96611020  00000000 00000000 00000000 00000000
fffff800`96611030  00000000 00000000 00000000 000000f8
fffff800`96611040  0eba1f0e cd09b400 4c01b821 685421cd
fffff800`96611050  70207369 72676f72 63206d61 6f6e6e61
fffff800`96611060  65622074 6e757220 206e6920 20534f44
fffff800`96611070  65646f6d 0a0d0d2e 00000024 00000000
0: kd> dd nt+4c
fffff800`9661104c  685421cd 70207369 72676f72 63206d61
fffff800`9661105c  6f6e6e61 65622074 6e757220 206e6920
fffff800`9661106c  20534f44 65646f6d 0a0d0d2e 00000024
fffff800`9661107c  00000000 562b5fbd 05453ef9 05453ef9
fffff800`9661108c  05453ef9 05fc4905 05453ef5 05443ef9
fffff800`9661109c  05453e9c 05453ef9 05453e9c 05d646f0
fffff800`966110ac  05453ef0 05f94905 05453e97 05fe4905
fffff800`966110bc  05453ec5 05f84905 05453ee2 05804905
0: kd>
```

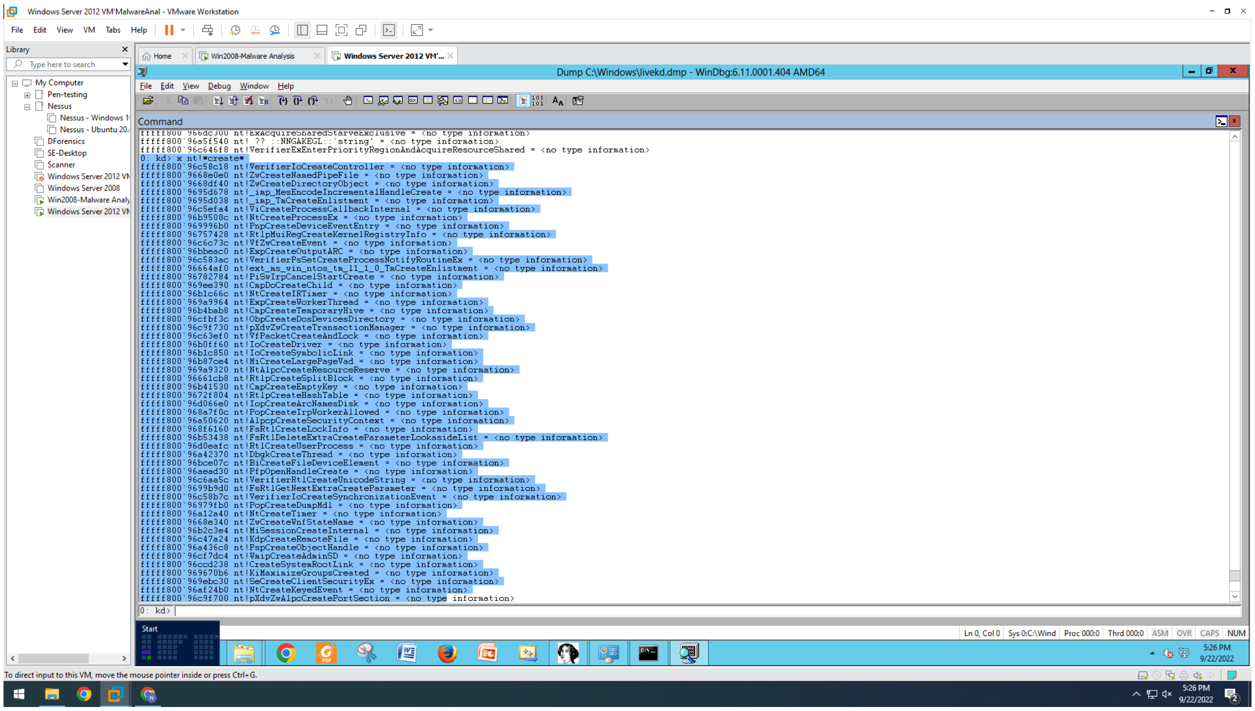
Viewing Memory

- In WinDbg, execute “dd nt”.
- Type “da nt”, “da nt+4c” and save a screenshot.



Windows Server 2012 VM'MalwareAnal - VMware Workstation
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
Command
Server Manager
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
fffff800`966110bc  05453ec5 05f84905 05453ee2 05804905
0: kd> x nt!*
fffff800`96cdfca8 nt!MxPageAlwaysHot = <no type information>
fffff800`966666a0 nt!MiSyncSystemPdes = <no type information>
fffff800`967cc530 nt!EtwTraceObjectOperation = <no type information>
fffff800`967375b0 nt!MiProcessWsInSwapRanges = <no type information>
fffff800`969a7030 nt!RtlSetOwnerSecurityDescriptor = <no type information>
fffff800`96a182bc nt!AlpcpDeleteBlob = <no type information>
fffff800`96cd4690 nt!IopStoreArcInformation = <no type information>
fffff800`9661756c nt!CcSetLoggedDataThreshold = <no type information>
fffff800`96b445b0 nt!CmpUpdateParentForEachSon = <no type information>
fffff800`96a88780 nt!PsReferenceImpersonationToken = <no type information>
fffff800`966ba2d0 nt!PpmSnapPerformanceAccumulation = <no type information>
fffff800`9670be10 nt! ?? ::FNODOBFM::`string' = <no type information>
fffff800`96a529e0 nt!EtwpUmglProviders = <no type information>
fffff800`966c9c20 nt!KiSetPriorityThread = <no type information>
fffff800`96b435d0 nt!CmpQueueLazyCommitWorker = <no type information>
fffff800`96685d80 nt!KiInterruptDispatchNoEOI = <no type information>
fffff800`96c58c18 nt!VerifierIoCreateController = <no type information>
fffff800`9664ea2c nt!RtlFindLastBackwardRunClear = <no type information>
fffff800`966998f0 nt!_newclmap = <no type information>
fffff800`96890720 nt!_lc_codepage = <no type information>
fffff800`96ac9518 nt!PopQueueBatteryStatusTimeout = <no type information>
fffff800`96acef98 nt!ExpGetSystemFirmwareTableInformation = <no type information>
fffff800`96bae864 nt!SmKmSendDeviceControl = <no type information>
fffff800`96c7b080 nt!ViEnableAfterHibernate = <no type information>
fffff800`969672b4 nt!PspJobNoWakeChargeLimit = <no type information>
fffff800`9668f640 nt!ZwRenameTransactionManager = <no type information>
fffff800`96c5faa4 nt!ViShutdownWatchdogExecuteDpc = <no type information>
fffff800`96bd0850 nt!BiAddBootEntryToNvramDisplayOrder = <no type information>
fffff800`968aed7c nt!MmZeroedPageSingleBitErrorsDetected = <no type information>
fffff800`96778f6c nt!InbvEnableBootDriver = <no type information>
fffff800`96afd778 nt!RegRtlOpenPredefinedKey = <no type information>
fffff800`96a0a790 nt!PsReturnProcessPageFileQuota = <no type information>
fffff800`96a553f8 nt! ?? ::LBKOJDO::`string' = <no type information>
fffff800`967b4f08 nt!B_TREE<unsigned long,ST_STORE<SM_TRAITS>::_ST_REGION_ENTRY,4096,NP_CONTEXT>::BTreeInsertEx = <no type information>
fffff800`96c77af4 nt!AnFwpDisableProgressTimer = <no type information>
fffff800`96b293b0 nt!BiIsVolumePartitionInformationRetained = <no type information>
fffff800`9670d240 nt! ?? ::FNODOBFM::`string' = <no type information>
fffff800`967c4888 nt!SMKM_STORE_MGR<SM_TRAITS>::SmStoreContentsRundown = <no type information>
fffff800`966cf0d0 nt!IoSetTopLevelIrp = <no type information>
fffff800`96622a8c nt!CcFlushCacheToLsn = <no type information>
fffff800`96972224 nt!PoBroadcastSystemState = <no type information>
fffff800`966adeb0 nt!DEVPKEY_Device_BusRelations = <no type information>
fffff800`96acb8d0 nt!PspAllocateAndQueryNotificationChannel = <no type information>
fffff800`96890a60 nt!WheapPfaLock = <no type information>
fffff800`96bc48f0 nt!ExUnregisterExtension = <no type information>
                                 vBusInformation = <no type information>
                                 BandwidthContract = <no type information>
                                 aProviderPnpidGuid = <no type information>
                                 BOPGDP::`string' = <no type information>
                                 erateRelations = <no type information>
                                 aseResourceForThreadLite = <no type information>
                                 encePageRuns = <no type information>
                                 dNextNamedTag = <no type information>
                                 VerifyService = <no type information>
```

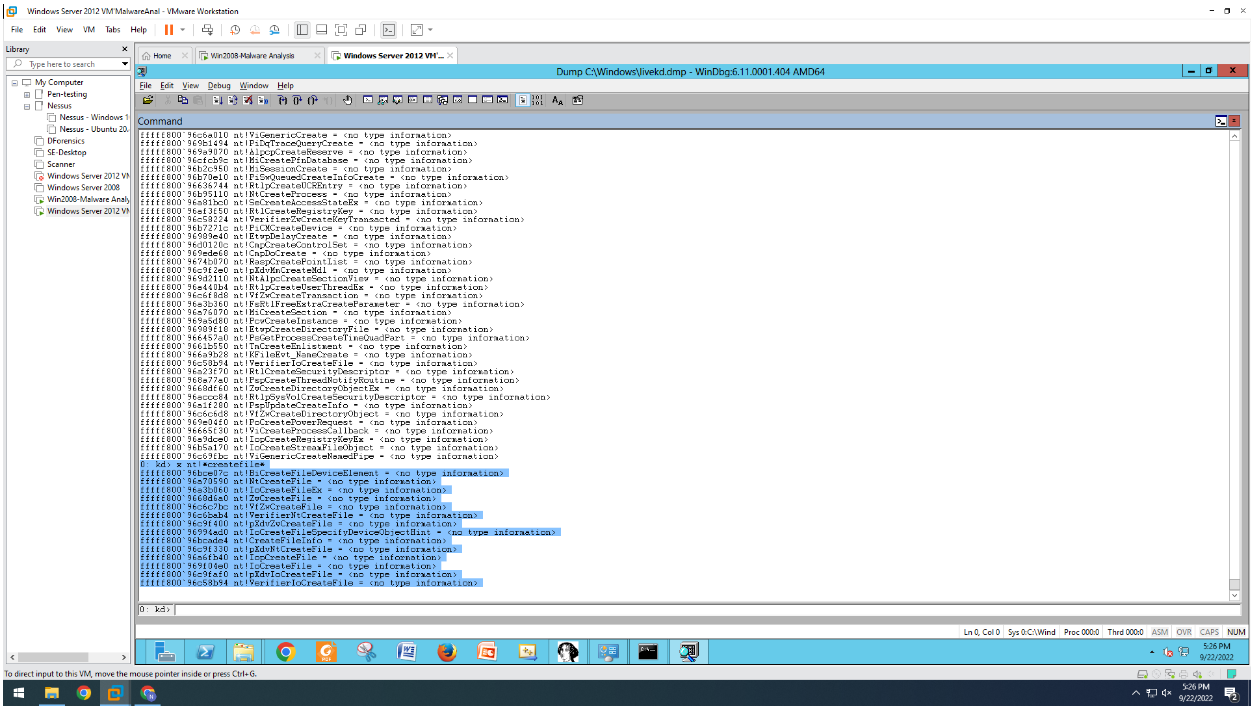


Windows Server 2012 VM'MalwareAnal - VMware Workstation
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
Command
Start
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

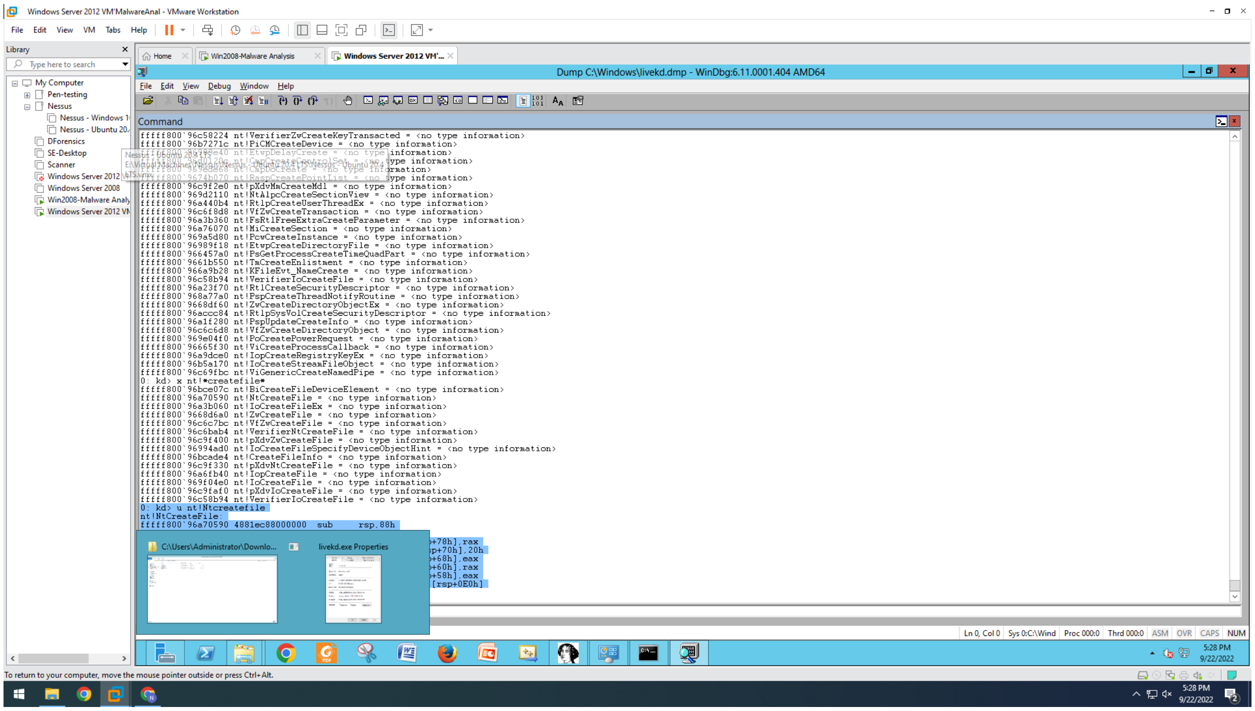
```
fffff800`966dc300 nt!ExAcquireSharedStarveExclusive = <no type information>
fffff800`96a5f540 nt! ?? ::NNGAKEGL::`string' = <no type information>
fffff800`96c646f8 nt!VerifierExEnterPriorityRegionAndAcquireResourceShared = <no type information>
0: kd> x nt!*create*
fffff800`96c58c18 nt!VerifierIoCreateController = <no type information>
fffff800`9668e0e0 nt!ZwCreateNamedPipeFile = <no type information>
fffff800`9668df40 nt!ZwCreateDirectoryObject = <no type information>
fffff800`9695d678 nt!_imp_MesEncodeIncrementalHandleCreate = <no type information>
fffff800`9695d038 nt!_imp_TmCreateEnlistment = <no type information>
fffff800`96c5efa4 nt!ViCreateProcessCallbackInternal = <no type information>
fffff800`96b9508c nt!NtCreateProcessEx = <no type information>
fffff800`969996b0 nt!PnpCreateDeviceEventEntry = <no type information>
fffff800`96757428 nt!RtlpMuiRegCreateKernelRegistryInfo = <no type information>
fffff800`96c6c73c nt!VfZwCreateEvent = <no type information>
fffff800`96bbeac0 nt!ExpCreateOutputARC = <no type information>
fffff800`96c583ac nt!VerifierPsSetCreateProcessNotifyRoutineEx = <no type information>
fffff800`96664af0 nt!ext_ms_win_ntos_tm_l1_1_0_TmCreateEnlistment = <no type information>
fffff800`96782784 nt!PiSwIrpCancelStartCreate = <no type information>
fffff800`969ee390 nt!CmpDoCreateChild = <no type information>
fffff800`96b1c66c nt!NtCreateIRTimer = <no type information>
fffff800`969a9964 nt!ExpCreateWorkerThread = <no type information>
fffff800`96b4bab8 nt!CmpCreateTemporaryHive = <no type information>
fffff800`96cfbf3c nt!ObpCreateDosDevicesDirectory = <no type information>
fffff800`96c9f730 nt!pXdvZwCreateTransactionManager = <no type information>
fffff800`96c63ef0 nt!VfPacketCreateAndLock = <no type information>
fffff800`96b0ff60 nt!IoCreateDriver = <no type information>
fffff800`96b1c850 nt!IoCreateSymbolicLink = <no type information>
fffff800`96b87ce4 nt!MiCreateLargePageVad = <no type information>
fffff800`969a9320 nt!NtAlpcCreateResourceReserve = <no type information>
fffff800`96661cb8 nt!RtlpCreateSplitBlock = <no type information>
fffff800`96b41530 nt!CmpCreateEmptyKey = <no type information>
fffff800`9672f804 nt!RtlpCreateHashTable = <no type information>
fffff800`96d066e0 nt!IopCreateArcNamesDisk = <no type information>
fffff800`968a7f0c nt!PopCreateIrpWorkerAllowed = <no type information>
fffff800`96a50620 nt!AlpcpCreateSecurityContext = <no type information>
fffff800`968f6160 nt!FsRtlCreateLockInfo = <no type information>
fffff800`96b53438 nt!FsRtlDeleteExtraCreateParameterLookasideList = <no type information>
fffff800`96d0eafc nt!RtlCreateUserProcess = <no type information>
fffff800`96a42370 nt!DbgkCreateThread = <no type information>
fffff800`96bce07c nt!BiCreateFileDeviceElement = <no type information>
fffff800`96aead30 nt!PfpOpenHandleCreate = <no type information>
fffff800`96c6aa5c nt!VerifierRtlCreateUnicodeString = <no type information>
fffff800`9699b9d0 nt!FsRtlGetNextExtraCreateParameter = <no type information>
fffff800`96c58b7c nt!VerifierIoCreateSynchronizationEvent = <no type information>
fffff800`96979fb0 nt!PopCreateDumpMdl = <no type information>
fffff800`96a12a40 nt!NtCreateTimer = <no type information>
fffff800`9668e340 nt!ZwCreateWnfStateName = <no type information>
fffff800`96b2c3e4 nt!MiSessionCreateInternal = <no type information>
fffff800`96c47a24 nt!KdpCreateRemoteFile = <no type information>
fffff800`96a436c8 nt!PspCreateObjectHandle = <no type information>
fffff800`96cf7dc4 nt!WmipCreateAdminSD = <no type information>
fffff800`96ccd238 nt!CreateSystemRootLink = <no type information>
fffff800`969670b6 nt!KiMaximizeGroupsCreated = <no type information>
fffff800`969ebc30 nt!SeCreateClientSecurityEx = <no type information>
fffff800`96af24b0 nt!NtCreateKeyedEvent = <no type information>
fffff800`96c9f700 nt!pXdvZwAlpcCreatePortSection = <no type information>
0: kd>
```

Searching for functions

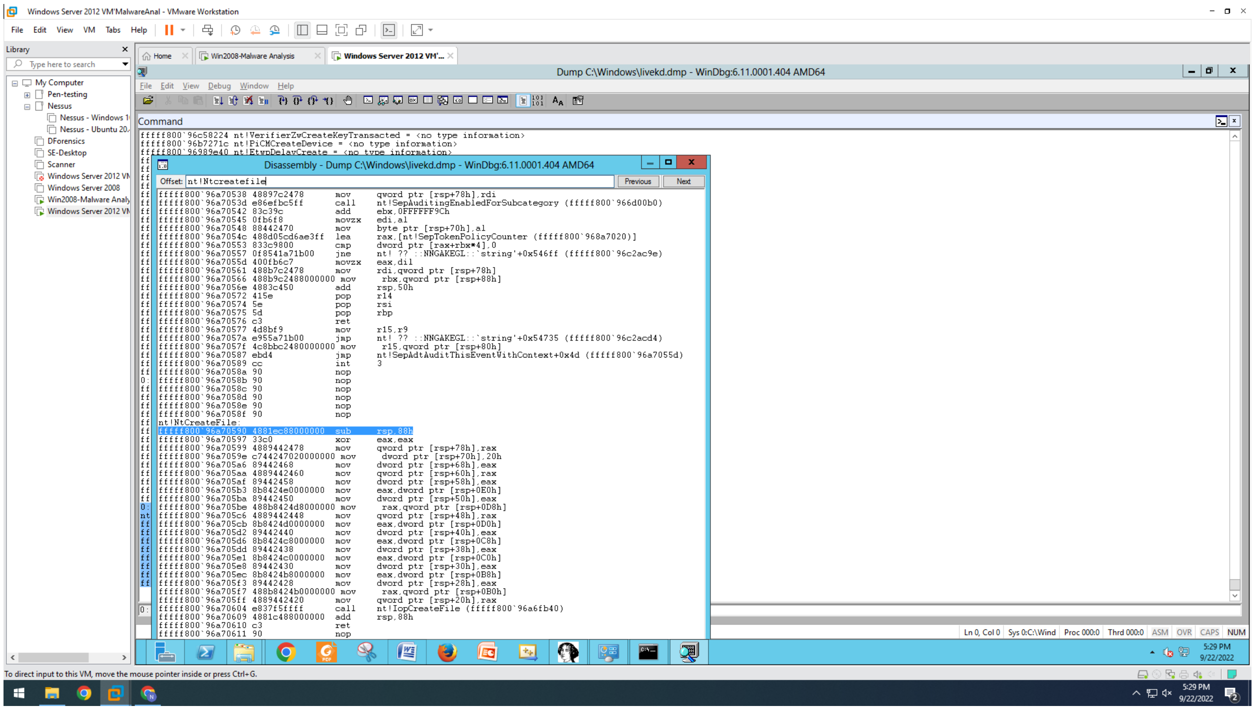
- Type “x nt!*”.
- Then “x nt!*Create*”, “x nt!*CreateFile*”.


Windows Server 2012 VM'MalwareAnal - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Pen-testing
Nessus
Nessus - Windows 1
Nessus - Ubuntu 20.
DForensics
SE-Desktop
Scanner
Windows Server 2012 VM
Windows Server 2008
Win2008-Malware Analy
Windows Server 2012 VM
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
File Edit View Debug Window Help
Command
Ln 0, Col 0 Sys 0:C:\Wind Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM
5:26 PM
9/22/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
fffff800`96c6a010 nt!ViGenericCreate = <no type information>
fffff800`969b1494 nt!PiDqTraceQueryCreate = <no type information>
fffff800`969a9070 nt!AlpcpCreateReserve = <no type information>
fffff800`96cfcb9c nt!MiCreatePfnDatabase = <no type information>
fffff800`96b2c950 nt!MiSessionCreate = <no type information>
fffff800`96b70e10 nt!PiSwQueuedCreateInfoCreate = <no type information>
fffff800`96636744 nt!RtlpCreateUCREntry = <no type information>
fffff800`96b95110 nt!NtCreateProcess = <no type information>
fffff800`96a81bc0 nt!SeCreateAccessStateEx = <no type information>
fffff800`96af3f50 nt!RtlCreateRegistryKey = <no type information>
fffff800`96c58224 nt!VerifierZwCreateKeyTransacted = <no type information>
fffff800`96b7271c nt!PiCMCreateDevice = <no type information>
fffff800`96989e40 nt!EtwpDelayCreate = <no type information>
fffff800`96d0120c nt!CmpCreateControlSet = <no type information>
fffff800`969ede68 nt!CmpDoCreate = <no type information>
fffff800`9674b070 nt!RaspCreatePointList = <no type information>
fffff800`96c9f2e0 nt!pXdvMmCreateMdl = <no type information>
fffff800`969d2110 nt!NtAlpcCreateSectionView = <no type information>
fffff800`96a440b4 nt!RtlpCreateUserThreadEx = <no type information>
fffff800`96c6f8d8 nt!VfZwCreateTransaction = <no type information>
fffff800`96a3b360 nt!FsRtlFreeExtraCreateParameter = <no type information>
fffff800`96a76070 nt!MiCreateSection = <no type information>
fffff800`969a5d80 nt!PcwCreateInstance = <no type information>
fffff800`96989f18 nt!EtwpCreateDirectoryFile = <no type information>
fffff800`966457a0 nt!PsGetProcessCreateTimeQuadPart = <no type information>
fffff800`9661b550 nt!TmCreateEnlistment = <no type information>
fffff800`966a9b28 nt!KFileEvt_NameCreate = <no type information>
fffff800`96c58b94 nt!VerifierIoCreateFile = <no type information>
fffff800`96a23f70 nt!RtlCreateSecurityDescriptor = <no type information>
fffff800`968a77a0 nt!PspCreateThreadNotifyRoutine = <no type information>
fffff800`9668df60 nt!ZwCreateDirectoryObjectEx = <no type information>
fffff800`96accc84 nt!RtlpSysVolCreateSecurityDescriptor = <no type information>
fffff800`96a1f280 nt!PspUpdateCreateInfo = <no type information>
fffff800`96c6c6d8 nt!VfZwCreateDirectoryObject = <no type information>
fffff800`969e04f0 nt!PoCreatePowerRequest = <no type information>
fffff800`96665f30 nt!ViCreateProcessCallback = <no type information>
fffff800`96a9dce0 nt!IopCreateRegistryKeyEx = <no type information>
fffff800`96b5a170 nt!IoCreateStreamFileObject = <no type information>
fffff800`96c69fbc nt!ViGenericCreateNamedPipe = <no type information>
0: kd> x nt!*createfile*
fffff800`96bce07c nt!BiCreateFileDeviceElement = <no type information>
fffff800`96a70590 nt!NtCreateFile = <no type information>
fffff800`96a3b060 nt!IoCreateFileEx = <no type information>
fffff800`9668d6a0 nt!ZwCreateFile = <no type information>
fffff800`96c6c7bc nt!VfZwCreateFile = <no type information>
fffff800`96c6bab4 nt!VerifierNtCreateFile = <no type information>
fffff800`96c9f400 nt!pXdvZwCreateFile = <no type information>
fffff800`96994ad0 nt!IoCreateFileSpecifyDeviceObjectHint = <no type information>
fffff800`96bcade4 nt!CreateFileInfo = <no type information>
fffff800`96c9f330 nt!pXdvNtCreateFile = <no type information>
fffff800`96a6fb40 nt!IopCreateFile = <no type information>
fffff800`969f04e0 nt!IoCreateFile = <no type information>
fffff800`96c9faf0 nt!pXdvIoCreateFile = <no type information>
fffff800`96c58b94 nt!VerifierIoCreateFile = <no type information>

0: kd>
```


Windows Server 2012 VM'MalwareAnal - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Pen-testing
Nessus
Nessus - Windows 1
Nessus - Ubuntu 20.
DForensics
SE-Desktop
Scanner
Windows Server 2012 VM
Windows Server 2008
Win2008-Malware Analy
Windows Server 2012 VM
Nessus - Ubuntu 20.4 LTS
E:\Virtual Machines\Nessus\Nessus - Ubuntu 20.4 LTS\Nessus - Ubuntu 20.4 LTS.vmx
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
File Edit View Debug Window Help
Command
C:\Users\Administrator\Downlo...
livekd.exe Properties
Ln 0, Col 0 Sys 0:C:\Wind Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM
5:28 PM
9/22/2022
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
fffff800`96c58224 nt!VerifierZwCreateKeyTransacted = <no type information>
fffff800`96b7271c nt!PiCMCreateDevice = <no type information>
fffff800`96989e40 nt!EtwpDelayCreate = <no type information>
fffff800`96d0120c nt!CmpCreateControlSet = <no type information>
fffff800`969ede68 nt!CmpDoCreate = <no type information>
fffff800`9674b070 nt!RaspCreatePointList = <no type information>
fffff800`96c9f2e0 nt!pXdvMmCreateMdl = <no type information>
fffff800`969d2110 nt!NtAlpcCreateSectionView = <no type information>
fffff800`96a440b4 nt!RtlpCreateUserThreadEx = <no type information>
fffff800`96c6f8d8 nt!VfZwCreateTransaction = <no type information>
fffff800`96a3b360 nt!FsRtlFreeExtraCreateParameter = <no type information>
fffff800`96a76070 nt!MiCreateSection = <no type information>
fffff800`969a5d80 nt!PcwCreateInstance = <no type information>
fffff800`96989f18 nt!EtwpCreateDirectoryFile = <no type information>
fffff800`966457a0 nt!PsGetProcessCreateTimeQuadPart = <no type information>
fffff800`9661b550 nt!TmCreateEnlistment = <no type information>
fffff800`966a9b28 nt!KFileEvt_NameCreate = <no type information>
fffff800`96c58b94 nt!VerifierIoCreateFile = <no type information>
fffff800`96a23f70 nt!RtlCreateSecurityDescriptor = <no type information>
fffff800`968a77a0 nt!PspCreateThreadNotifyRoutine = <no type information>
fffff800`9668df60 nt!ZwCreateDirectoryObjectEx = <no type information>
fffff800`96accc84 nt!RtlpSysVolCreateSecurityDescriptor = <no type information>
fffff800`96a1f280 nt!PspUpdateCreateInfo = <no type information>
fffff800`96c6c6d8 nt!VfZwCreateDirectoryObject = <no type information>
fffff800`969e04f0 nt!PoCreatePowerRequest = <no type information>
fffff800`96665f30 nt!ViCreateProcessCallback = <no type information>
fffff800`96a9dce0 nt!IopCreateRegistryKeyEx = <no type information>
fffff800`96b5a170 nt!IoCreateStreamFileObject = <no type information>
fffff800`96c69fbc nt!ViGenericCreateNamedPipe = <no type information>
0: kd> x nt!*createfile*
fffff800`96bce07c nt!BiCreateFileDeviceElement = <no type information>
fffff800`96a70590 nt!NtCreateFile = <no type information>
fffff800`96a3b060 nt!IoCreateFileEx = <no type information>
fffff800`9668d6a0 nt!ZwCreateFile = <no type information>
fffff800`96c6c7bc nt!VfZwCreateFile = <no type information>
fffff800`96c6bab4 nt!VerifierNtCreateFile = <no type information>
fffff800`96c9f400 nt!pXdvZwCreateFile = <no type information>
fffff800`96994ad0 nt!IoCreateFileSpecifyDeviceObjectHint = <no type information>
fffff800`96bcade4 nt!CreateFileInfo = <no type information>
fffff800`96c9f330 nt!pXdvNtCreateFile = <no type information>
fffff800`96a6fb40 nt!IopCreateFile = <no type information>
fffff800`969f04e0 nt!IoCreateFile = <no type information>
fffff800`96c9faf0 nt!pXdvIoCreateFile = <no type information>
fffff800`96c58b94 nt!VerifierIoCreateFile = <no type information>
0: kd> u nt!Ntcreatefile
nt!NtCreateFile:
fffff800`96a70590 4881ec88000000  sub     rsp,88h
                                                  +78h],rax
                                                  p+70h],20h
                                                  +68h],eax
                                                  +60h],rax
                                                  +58h],eax
                                                   [rsp+0E0h]
```


Windows Server 2012 VM'MalwareAnal - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Pen-testing
Nessus
Nessus - Windows 1
Nessus - Ubuntu 20.
DForensics
SE-Desktop
Scanner
Windows Server 2012 VM
Windows Server 2008
Win2008-Malware Analy
Windows Server 2012 VM
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
File Edit View Debug Window Help
Command
Disassembly - Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
Previous
Next
Ln 0, Col 0 Sys 0:C:\Wind Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM
5:29 PM
9/22/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5:29 PM
9/22/2022

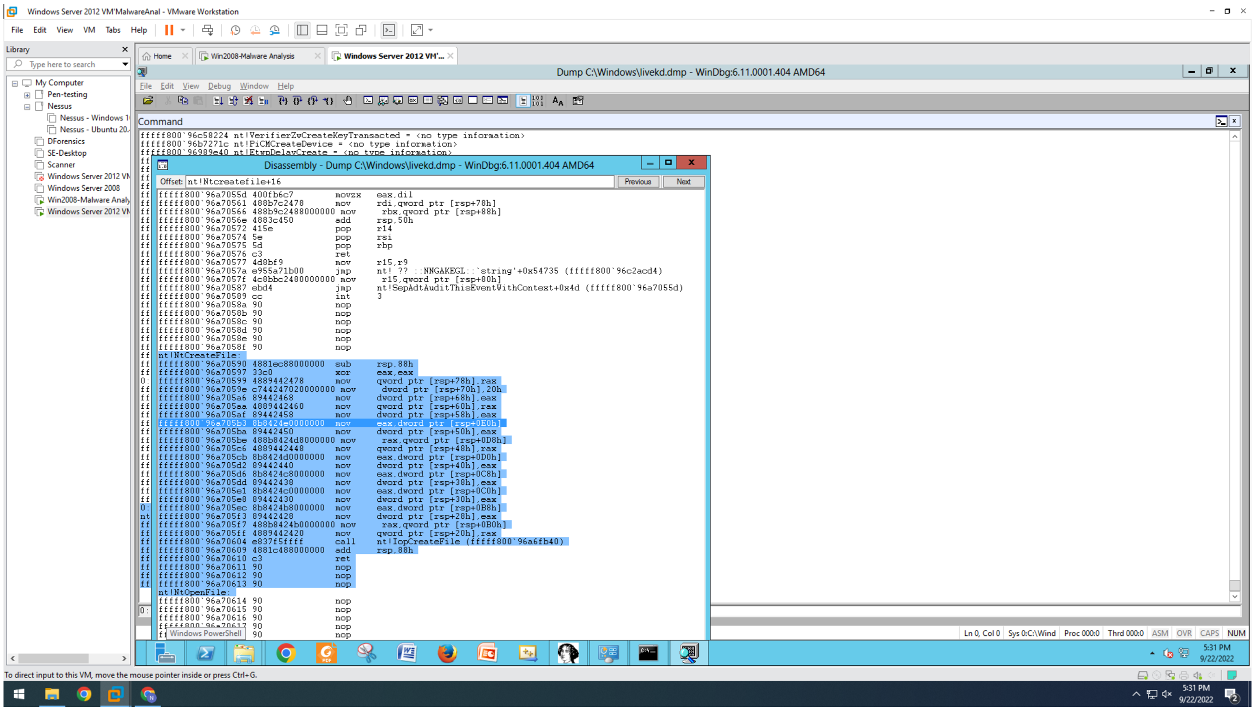
```
fffff800`96c58224 nt!VerifierZwCreateKeyTransacted = <no type information>
fffff800`96b7271c nt!PiCMCreateDevice = <no type information>
fffff800`96989e40 nt!EtwpDelayCreate = <no type information>
```

Offset: nt!Ntcreatefile

```
fffff800`96a70538 48897c2478       mov     qword ptr [rsp+78h],rdi
fffff800`96a7053d e86efbc5ff       call    nt!SepAuditingEnabledForSubcategory (fffff800`966d00b0)
fffff800`96a70542 83c39c           add     ebx,0FFFFFF9Ch
fffff800`96a70545 0fb6f8           movzx   edi,al
fffff800`96a70548 88442470         mov     byte ptr [rsp+70h],al
fffff800`96a7054c 488d05cd6ae3ff   lea     rax,[nt!SepTokenPolicyCounter (fffff800`968a7020)]
fffff800`96a70553 833c9800         cmp     dword ptr [rax+rbx*4],0
fffff800`96a70557 0f8541a71b00     jne     nt! ?? ::NNGAKEGL::`string'+0x546ff (fffff800`96c2ac9e)
fffff800`96a7055d 400fb6c7         movzx   eax,dil
fffff800`96a70561 488b7c2478       mov     rdi,qword ptr [rsp+78h]
fffff800`96a70566 488b9c2488000000 mov      rbx,qword ptr [rsp+88h]
fffff800`96a7056e 4883c450         add     rsp,50h
fffff800`96a70572 415e             pop     r14
fffff800`96a70574 5e               pop     rsi
fffff800`96a70575 5d               pop     rbp
fffff800`96a70576 c3               ret
fffff800`96a70577 4d8bf9           mov     r15,r9
fffff800`96a7057a e955a71b00       jmp     nt! ?? ::NNGAKEGL::`string'+0x54735 (fffff800`96c2acd4)
fffff800`96a7057f 4c8bbc2480000000 mov      r15,qword ptr [rsp+80h]
fffff800`96a70587 ebd4             jmp     nt!SepAdtAuditThisEventWithContext+0x4d (fffff800`96a7055d)
fffff800`96a70589 cc               int     3
fffff800`96a7058a 90               nop
fffff800`96a7058b 90               nop
fffff800`96a7058c 90               nop
fffff800`96a7058d 90               nop
fffff800`96a7058e 90               nop
fffff800`96a7058f 90               nop
nt!NtCreateFile:
fffff800`96a70590 4881ec88000000   sub     rsp,88h
fffff800`96a70597 33c0             xor     eax,eax
fffff800`96a70599 4889442478       mov     qword ptr [rsp+78h],rax
fffff800`96a7059e c744247020000000 mov      dword ptr [rsp+70h],20h
fffff800`96a705a6 89442468         mov     dword ptr [rsp+68h],eax
fffff800`96a705aa 4889442460       mov     qword ptr [rsp+60h],rax
fffff800`96a705af 89442458         mov     dword ptr [rsp+58h],eax
fffff800`96a705b3 8b8424e0000000   mov     eax,dword ptr [rsp+0E0h]
fffff800`96a705ba 89442450         mov     dword ptr [rsp+50h],eax
fffff800`96a705be 488b8424d8000000 mov      rax,qword ptr [rsp+0D8h]
fffff800`96a705c6 4889442448       mov     qword ptr [rsp+48h],rax
fffff800`96a705cb 8b8424d0000000   mov     eax,dword ptr [rsp+0D0h]
fffff800`96a705d2 89442440         mov     dword ptr [rsp+40h],eax
fffff800`96a705d6 8b8424c8000000   mov     eax,dword ptr [rsp+0C8h]
fffff800`96a705dd 89442438         mov     dword ptr [rsp+38h],eax
fffff800`96a705e1 8b8424c0000000   mov     eax,dword ptr [rsp+0C0h]
fffff800`96a705e8 89442430         mov     dword ptr [rsp+30h],eax
fffff800`96a705ec 8b8424b8000000   mov     eax,dword ptr [rsp+0B8h]
fffff800`96a705f3 89442428         mov     dword ptr [rsp+28h],eax
fffff800`96a705f7 488b8424b0000000 mov      rax,qword ptr [rsp+0B0h]
fffff800`96a705ff 4889442420       mov     qword ptr [rsp+20h],rax
fffff800`96a70604 e837f5ffff       call    nt!IopCreateFile (fffff800`96a6fb40)
fffff800`96a70609 4881c488000000   add     rsp,88h
fffff800`96a70610 c3               ret
fffff800`96a70611 90               nop
```

Unassembling a function

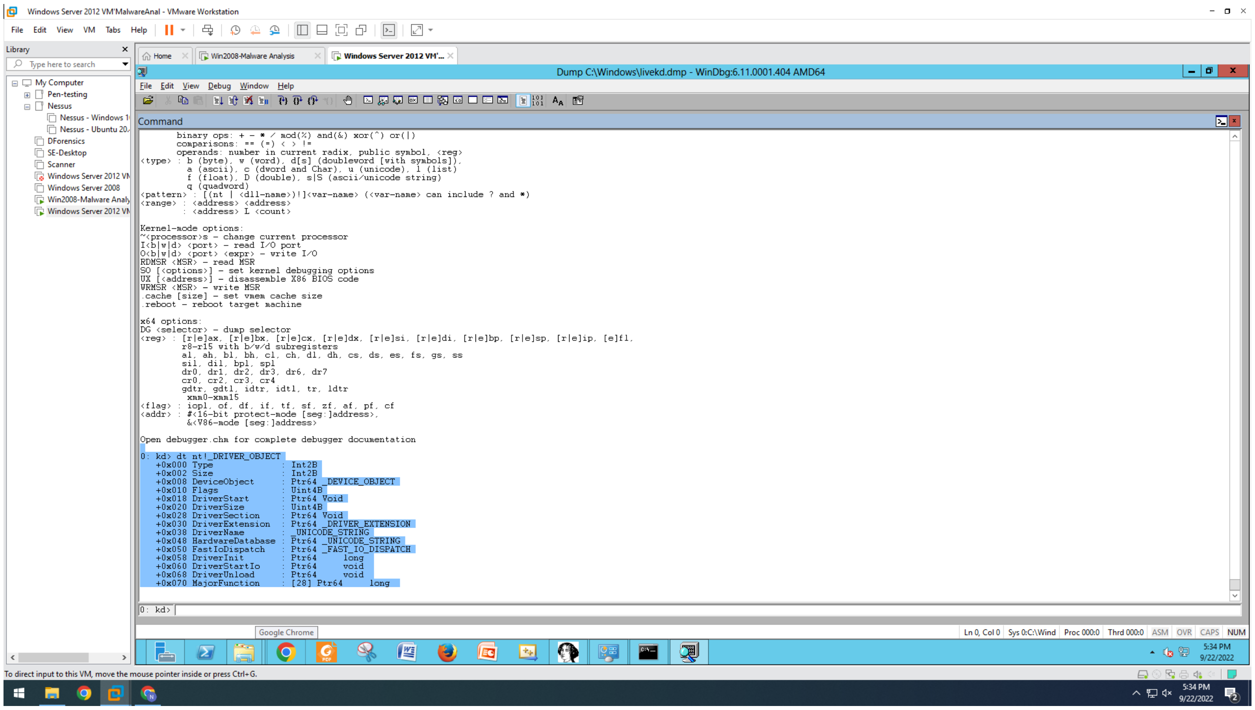
- Type “u n!NtCreateFile”.
- Then click view > Disassembly.
- And save a screen shot.


Windows Server 2012 VM'MalwareAnal - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Pen-testing
Nessus
Nessus - Windows 1
Nessus - Ubuntu 20.
DForensics
SE-Desktop
Scanner
Windows Server 2012 VM
Windows Server 2008
Win2008-Malware Analy
Windows Server 2012 VM
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
File Edit View Debug Window Help
Command
Disassembly - Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
Previous
Next
Windows PowerShell
Ln 0, Col 0 Sys 0:C:\Wind Proc 000:0 Thrd 000:0 ASM OVR CAPS NUM
5:31 PM
9/22/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5:31 PM
9/22/2022

```
fffff800`96c58224 nt!VerifierZwCreateKeyTransacted = <no type information>
fffff800`96b7271c nt!PiCMCreateDevice = <no type information>
fffff800`96989e40 nt!EtwpDelayCreate = <no type information>
```

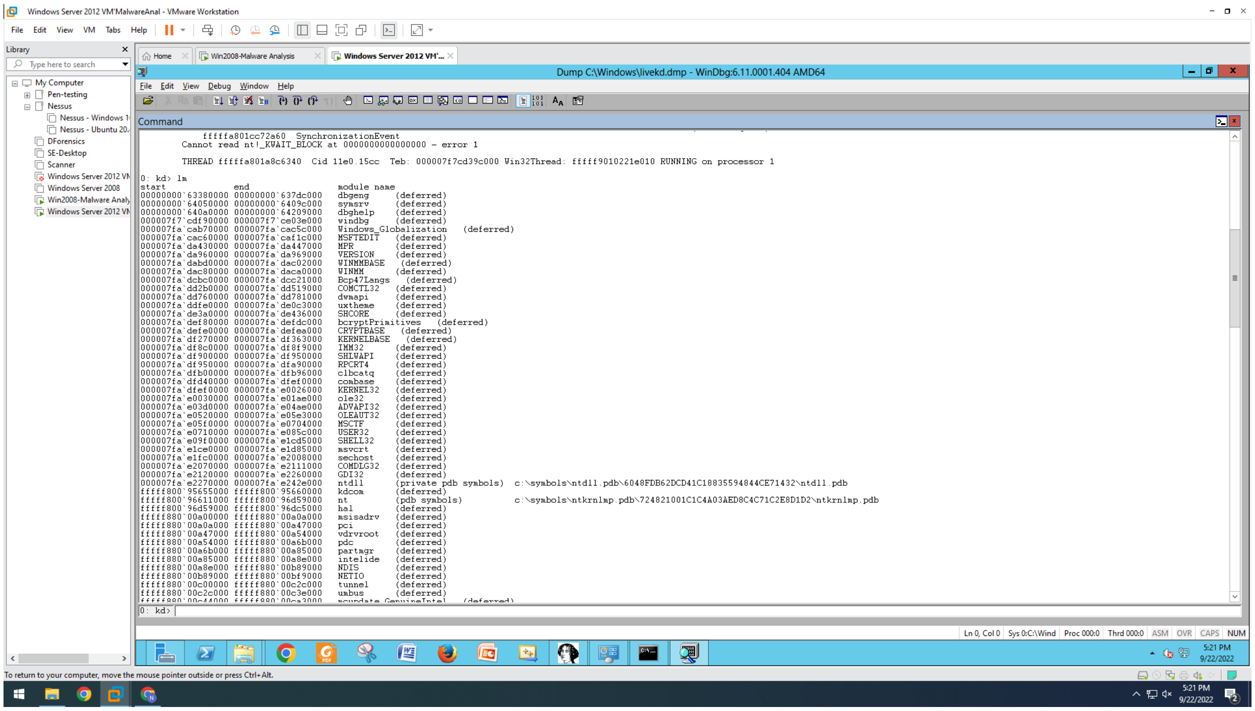
Offset: nt!Ntcreatefile+16

```
fffff800`96a7055d 400fb6c7         movzx   eax,dil
fffff800`96a70561 488b7c2478       mov     rdi,qword ptr [rsp+78h]
fffff800`96a70566 488b9c2488000000 mov      rbx,qword ptr [rsp+88h]
fffff800`96a7056e 4883c450         add     rsp,50h
fffff800`96a70572 415e             pop     r14
fffff800`96a70574 5e               pop     rsi
fffff800`96a70575 5d               pop     rbp
fffff800`96a70576 c3               ret
fffff800`96a70577 4d8bf9           mov     r15,r9
fffff800`96a7057a e955a71b00       jmp     nt! ?? ::NNGAKEGL::`string'+0x54735 (fffff800`96c2acd4)
fffff800`96a7057f 4c8bbc2480000000 mov      r15,qword ptr [rsp+80h]
fffff800`96a70587 ebd4             jmp     nt!SepAdtAuditThisEventWithContext+0x4d (fffff800`96a7055d)
fffff800`96a70589 cc               int     3
fffff800`96a7058a 90               nop
fffff800`96a7058b 90               nop
fffff800`96a7058c 90               nop
fffff800`96a7058d 90               nop
fffff800`96a7058e 90               nop
fffff800`96a7058f 90               nop
nt!NtCreateFile:
fffff800`96a70590 4881ec88000000   sub     rsp,88h
fffff800`96a70597 33c0             xor     eax,eax
fffff800`96a70599 4889442478       mov     qword ptr [rsp+78h],rax
fffff800`96a7059e c744247020000000 mov      dword ptr [rsp+70h],20h
fffff800`96a705a6 89442468         mov     dword ptr [rsp+68h],eax
fffff800`96a705aa 4889442460       mov     qword ptr [rsp+60h],rax
fffff800`96a705af 89442458         mov     dword ptr [rsp+58h],eax
fffff800`96a705b3 8b8424e0000000   mov     eax,dword ptr [rsp+0E0h]
fffff800`96a705ba 89442450         mov     dword ptr [rsp+50h],eax
fffff800`96a705be 488b8424d8000000 mov      rax,qword ptr [rsp+0D8h]
fffff800`96a705c6 4889442448       mov     qword ptr [rsp+48h],rax
fffff800`96a705cb 8b8424d0000000   mov     eax,dword ptr [rsp+0D0h]
fffff800`96a705d2 89442440         mov     dword ptr [rsp+40h],eax
fffff800`96a705d6 8b8424c8000000   mov     eax,dword ptr [rsp+0C8h]
fffff800`96a705dd 89442438         mov     dword ptr [rsp+38h],eax
fffff800`96a705e1 8b8424c0000000   mov     eax,dword ptr [rsp+0C0h]
fffff800`96a705e8 89442430         mov     dword ptr [rsp+30h],eax
fffff800`96a705ec 8b8424b8000000   mov     eax,dword ptr [rsp+0B8h]
fffff800`96a705f3 89442428         mov     dword ptr [rsp+28h],eax
fffff800`96a705f7 488b8424b0000000 mov      rax,qword ptr [rsp+0B0h]
fffff800`96a705ff 4889442420       mov     qword ptr [rsp+20h],rax
fffff800`96a70604 e837f5ffff       call    nt!IopCreateFile (fffff800`96a6fb40)
fffff800`96a70609 4881c488000000   add     rsp,88h
fffff800`96a70610 c3               ret
fffff800`96a70611 90               nop
fffff800`96a70612 90               nop
fffff800`96a70613 90               nop
nt!NtOpenFile:
fffff800`96a70614 90               nop
fffff800`96a70615 90               nop
fffff800`96a70616 90               nop
fffff800`96a70617 90               nop
                  90               nop
```



Windows Server 2012 VM'MalwareAnal - VMware Workstation
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
Command
Google Chrome
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
        binary ops: + - * / mod(%) and(&) xor(^) or(|)
        comparisons: == (=) < > !=
        operands: number in current radix, public symbol, <reg>
<type> : b (byte), w (word), d[s] (doubleword [with symbols]),
         a (ascii), c (dword and Char), u (unicode), l (list)
         f (float), D (double), s|S (ascii/unicode string)
         q (quadword)
<pattern> : [(nt | <dll-name>)!]<var-name> (<var-name> can include ? and *)
<range> : <address> <address>
        : <address> L <count>

Kernel-mode options:
~<processor>s - change current processor
I<b|w|d> <port> - read I/O port
O<b|w|d> <port> <expr> - write I/O
RDMSR <MSR> - read MSR
SO [<options>] - set kernel debugging options
UX [<address>] - disassemble X86 BIOS code
WRMSR <MSR> - write MSR
.cache [size] - set vmem cache size
.reboot - reboot target machine

x64 options:
DG <selector> - dump selector
<reg> : [r|e]ax, [r|e]bx, [r|e]cx, [r|e]dx, [r|e]si, [r|e]di, [r|e]bp, [r|e]sp, [r|e]ip, [e]fl,
        r8-r15 with b/w/d subregisters
        al, ah, bl, bh, cl, ch, dl, dh, cs, ds, es, fs, gs, ss
        sil, dil, bpl, spl
        dr0, dr1, dr2, dr3, dr6, dr7
        cr0, cr2, cr3, cr4
        gdtr, gdtl, idtr, idtl, tr, ldtr
         xmm0-xmm15
<flag> : iopl, of, df, if, tf, sf, zf, af, pf, cf
<addr> : #<16-bit protect-mode [seg:]address>,
         &<V86-mode [seg:]address>

Open debugger.chm for complete debugger documentation

0: kd> dt nt!_DRIVER_OBJECT
   +0x000 Type             : Int2B
   +0x002 Size             : Int2B
   +0x008 DeviceObject     : Ptr64 _DEVICE_OBJECT
   +0x010 Flags            : Uint4B
   +0x018 DriverStart      : Ptr64 Void
   +0x020 DriverSize       : Uint4B
   +0x028 DriverSection    : Ptr64 Void
   +0x030 DriverExtension  : Ptr64 _DRIVER_EXTENSION
   +0x038 DriverName       : _UNICODE_STRING
   +0x048 HardwareDatabase : Ptr64 _UNICODE_STRING
   +0x050 FastIoDispatch   : Ptr64 _FAST_IO_DISPATCH
   +0x058 DriverInit       : Ptr64     long
   +0x060 DriverStartIo    : Ptr64     void
   +0x068 DriverUnload     : Ptr64     void
   +0x070 MajorFunction    : [28] Ptr64     long

0: kd>
```



Windows Server 2012 VM'MalwareAnal - VMware Workstation
Home
Win2008-Malware Analysis
Windows Server 2012 VM'...
Dump C:\Windows\livekd.dmp - WinDbg:6.11.0001.404 AMD64
Command
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
            fffffa801cc72a60  SynchronizationEvent
        Cannot read nt!_KWAIT_BLOCK at 0000000000000000 - error 1

        THREAD fffffa801a8c6340  Cid 11e0.15cc  Teb: 000007f7cd39c000 Win32Thread: fffff9010221e010 RUNNING on processor 1

0: kd> lm
start             end                 module name
00000000`63380000 00000000`637dc000   dbgeng     (deferred)
00000000`64050000 00000000`6409c000   symsrv     (deferred)
00000000`640a0000 00000000`64209000   dbghelp    (deferred)
000007f7`cdf90000 000007f7`ce03e000   windbg     (deferred)
000007fa`cab70000 000007fa`cac5c000   Windows_Globalization   (deferred)
000007fa`cac60000 000007fa`caf1c000   MSFTEDIT   (deferred)
000007fa`da430000 000007fa`da447000   MPR        (deferred)
000007fa`da960000 000007fa`da969000   VERSION    (deferred)
000007fa`dabd0000 000007fa`dac02000   WINMMBASE   (deferred)
000007fa`dac80000 000007fa`daca0000   WINMM      (deferred)
000007fa`dcbc0000 000007fa`dcc21000   Bcp47Langs   (deferred)
000007fa`dd2b0000 000007fa`dd519000   COMCTL32   (deferred)
000007fa`dd760000 000007fa`dd781000   dwmapi     (deferred)
000007fa`ddfe0000 000007fa`de0c3000   uxtheme    (deferred)
000007fa`de3a0000 000007fa`de436000   SHCORE     (deferred)
000007fa`def80000 000007fa`defdc000   bcryptPrimitives   (deferred)
000007fa`defe0000 000007fa`defea000   CRYPTBASE   (deferred)
000007fa`df270000 000007fa`df363000   KERNELBASE   (deferred)
000007fa`df8c0000 000007fa`df8f9000   IMM32      (deferred)
000007fa`df900000 000007fa`df950000   SHLWAPI    (deferred)
000007fa`df950000 000007fa`dfa90000   RPCRT4     (deferred)
000007fa`dfb00000 000007fa`dfb96000   clbcatq    (deferred)
000007fa`dfd40000 000007fa`dfef0000   combase    (deferred)
000007fa`dfef0000 000007fa`e0026000   KERNEL32   (deferred)
000007fa`e0030000 000007fa`e01ae000   ole32      (deferred)
000007fa`e03d0000 000007fa`e04ae000   ADVAPI32   (deferred)
000007fa`e0520000 000007fa`e05e3000   OLEAUT32   (deferred)
000007fa`e05f0000 000007fa`e0704000   MSCTF      (deferred)
000007fa`e0710000 000007fa`e085c000   USER32     (deferred)
000007fa`e09f0000 000007fa`e1cd5000   SHELL32    (deferred)
000007fa`e1ce0000 000007fa`e1d85000   msvcrt     (deferred)
000007fa`e1fc0000 000007fa`e2008000   sechost    (deferred)
000007fa`e2070000 000007fa`e2111000   COMDLG32   (deferred)
000007fa`e2120000 000007fa`e2260000   GDI32      (deferred)
000007fa`e2270000 000007fa`e242e000   ntdll      (private pdb symbols)  c:\symbols\ntdll.pdb\6048FDB62DCD41C18835594844CE71432\ntdll.pdb
fffff800`95655000 fffff800`95660000   kdcom      (deferred)
fffff800`96611000 fffff800`96d59000   nt         (pdb symbols)          c:\symbols\ntkrnlmp.pdb\724821001C1C4A03AED8C4C71C2E8D1D2\ntkrnlmp.pdb
fffff800`96d59000 fffff800`96dc5000   hal        (deferred)
fffff880`00a00000 fffff880`00a0a000   msisadrv   (deferred)
fffff880`00a0a000 fffff880`00a47000   pci        (deferred)
fffff880`00a47000 fffff880`00a54000   vdrvroot   (deferred)
fffff880`00a54000 fffff880`00a6b000   pdc        (deferred)
fffff880`00a6b000 fffff880`00a85000   partmgr    (deferred)
fffff880`00a85000 fffff880`00a8e000   intelide   (deferred)
fffff880`00a8e000 fffff880`00b89000   NDIS       (deferred)
fffff880`00b89000 fffff880`00bf9000   NETIO      (deferred)
fffff880`00c00000 fffff880`00c2c000   tunnel     (deferred)
fffff880`00c2c000 fffff880`00c3e000   umbus      (deferred)
fffff880`00c44000 fffff880`00ca3000   mcupdate_GenuineIntel    (deferred)

0: kd>
```

<u>Conclusion</u>: To conclude with the lab, we learned how to debug Using Kernel Debugging Commands with WinDbg.