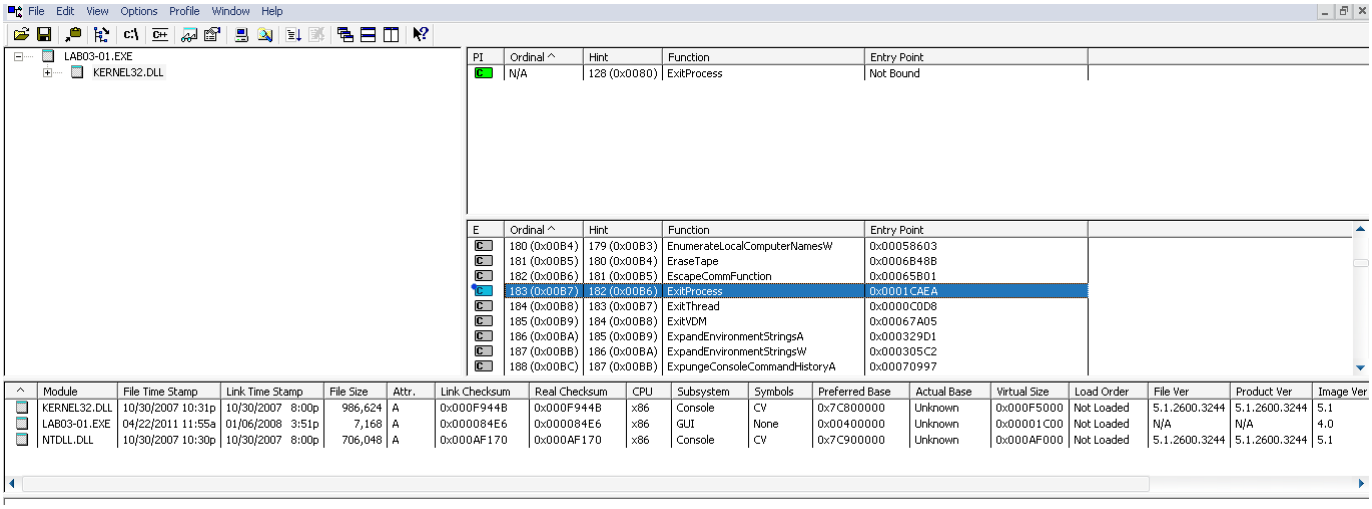
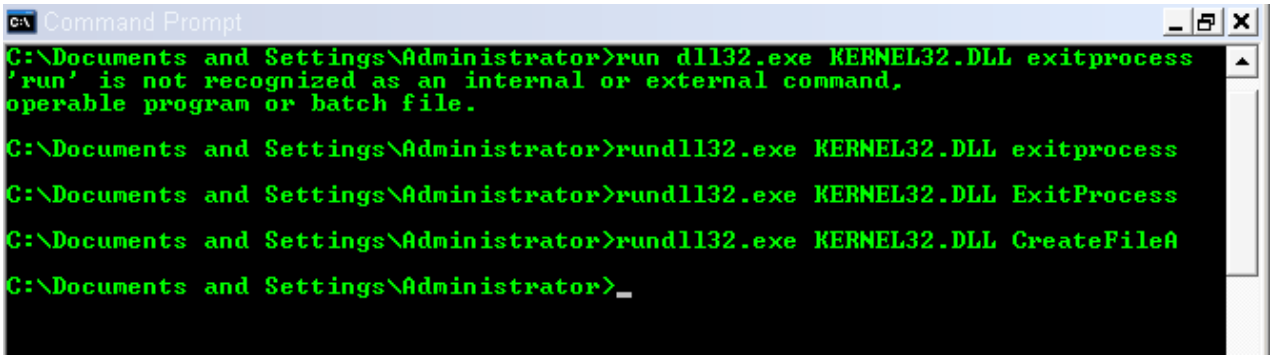
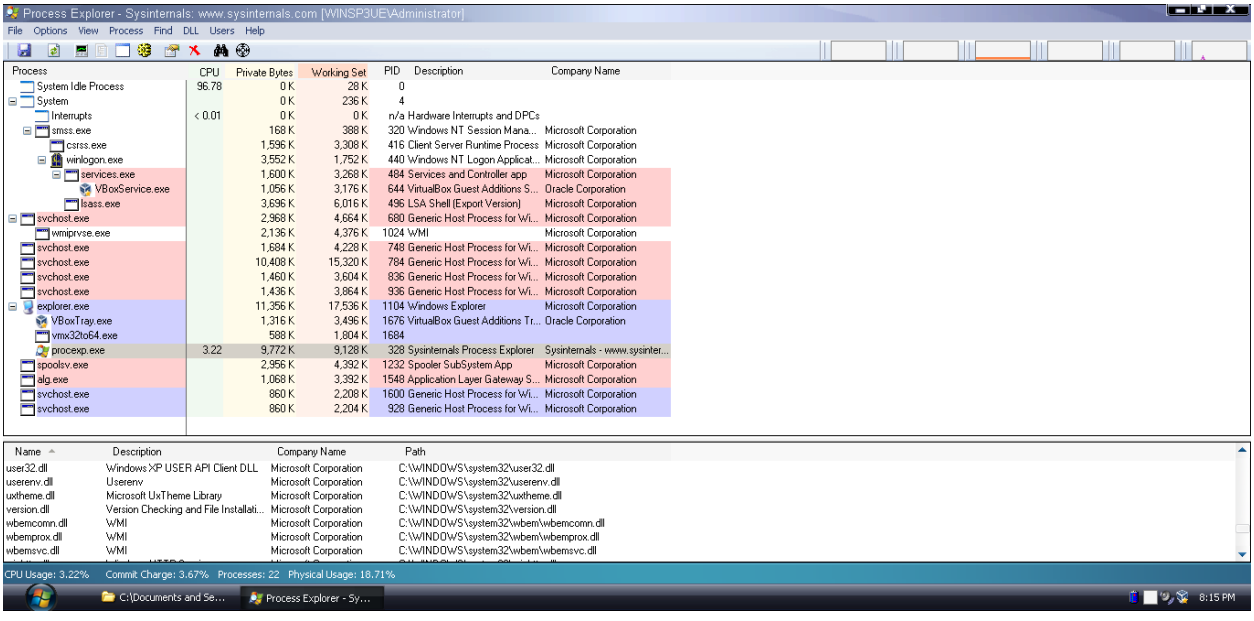
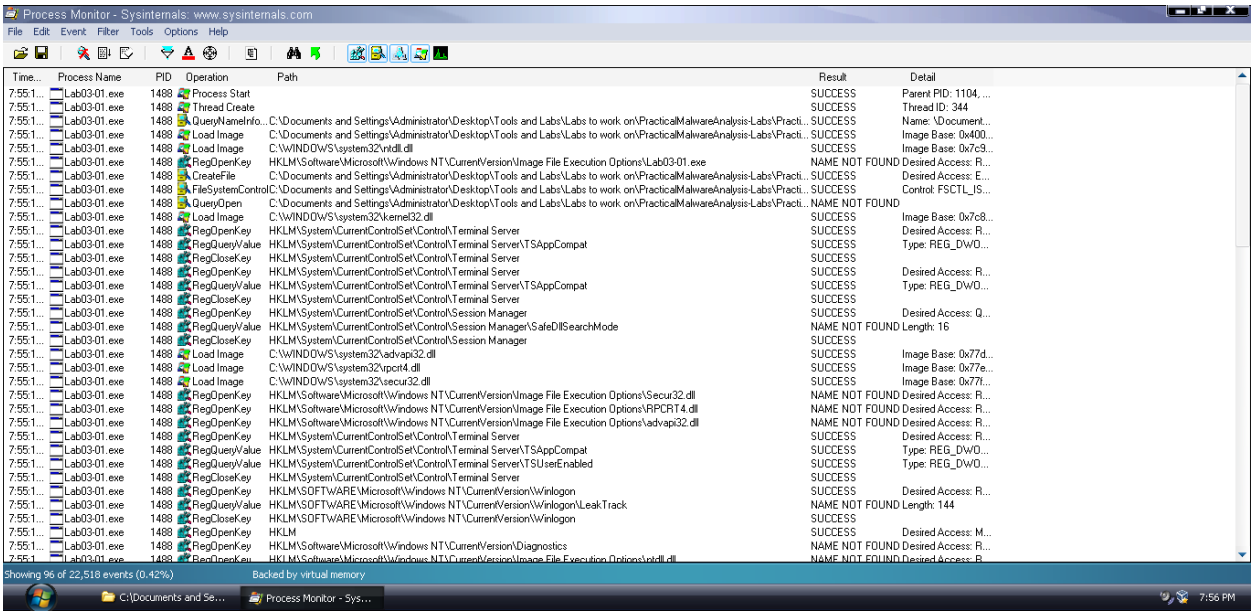
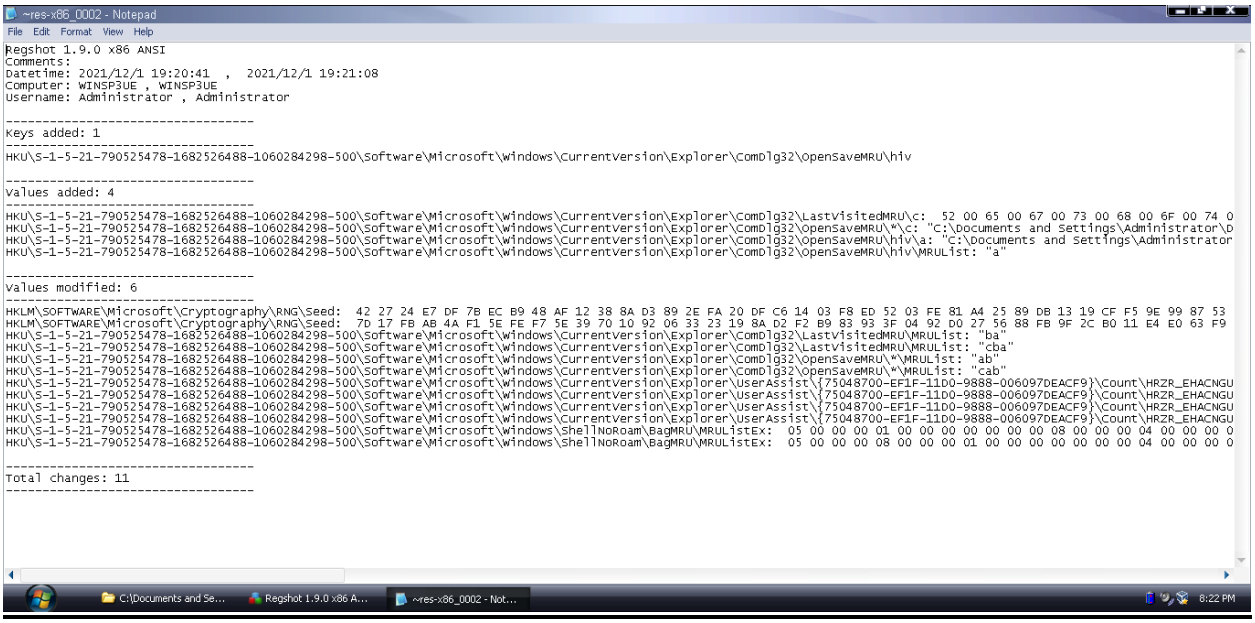
Lab 3-01


File Edit View Options Profile Window Help
LAB03-01.EXE
KERNEL32.DLL
PI Ordinal ^ Hint Function Entry Point
N/A 128 (0x0080) ExitProcess Not Bound
E Ordinal ^ Hint Function Entry Point
180 (0x00B4) 179 (0x00B3) EnumerateLocalComputerNamesW 0x00058603
181 (0x00B5) 180 (0x00B4) EraseTape 0x0006B48B
182 (0x00B6) 181 (0x00B5) EscapeCommFunction 0x00065B01
183 (0x00B7) 182 (0x00B6) ExitProcess 0x0001CAEA
184 (0x00B8) 183 (0x00B7) ExitThread 0x0000C0D8
185 (0x00B9) 184 (0x00B8) ExitVDM 0x00067A05
186 (0x00BA) 185 (0x00B9) ExpandEnvironmentStringsA 0x000329D1
187 (0x00BB) 186 (0x00BA) ExpandEnvironmentStringsW 0x000305C2
188 (0x00BC) 187 (0x00BB) ExpungeConsoleCommandHistoryA 0x00070997
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image Ver
KERNEL32.DLL 10/30/2007 10:31p 10/30/2007 8:00p 986,624 A 0x000F944B 0x000F944B x86 Console CV 0x7C800000 Unknown 0x000F5000 Not Loaded 5.1.2600.3244 5.1.2600.3244 5.1
LAB03-01.EXE 04/22/2011 11:55a 01/06/2008 3:51p 7,168 A 0x000084E6 0x000084E6 x86 GUI None 0x00400000 Unknown 0x00001C00 Not Loaded N/A N/A 4.0
NTDLL.DLL 10/30/2007 10:30p 10/30/2007 8:00p 706,048 A 0x000AF170 0x000AF170 x86 Console CV 0x7C900000 Unknown 0x000AF000 Not Loaded 5.1.2600.3244 5.1.2600.3244 5.1

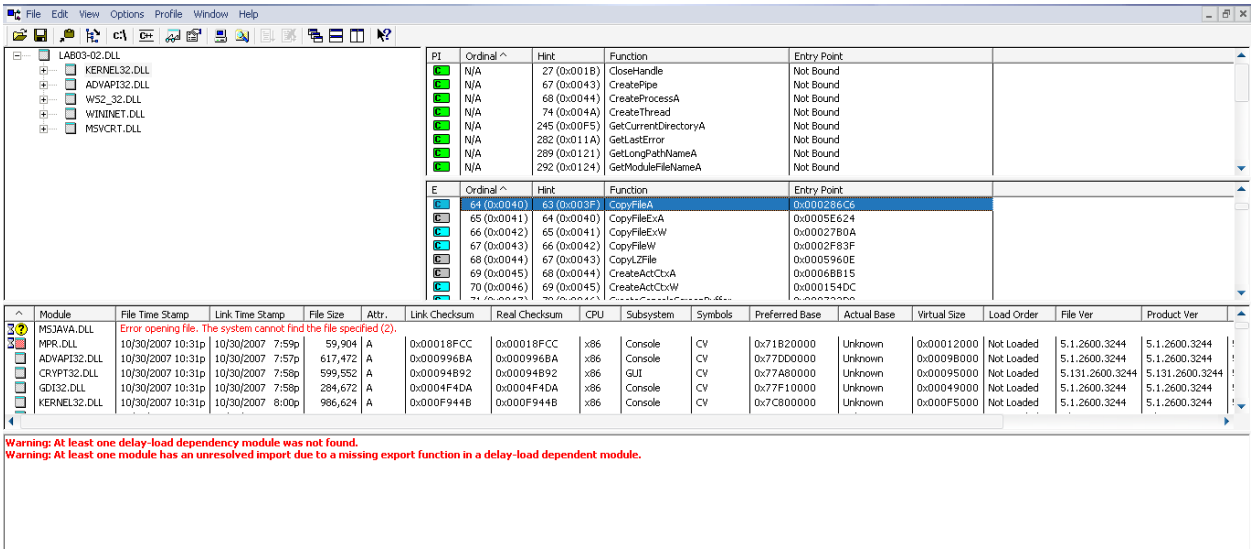

Command Prompt
C:\Documents and Settings\Administrator>run dll32.exe KERNEL32.DLL exitprocess
'run' is not recognized as an internal or external command,
operable program or batch file.
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL exitprocess
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL ExitProcess
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CreateFileA
C:\Documents and Settings\Administrator>

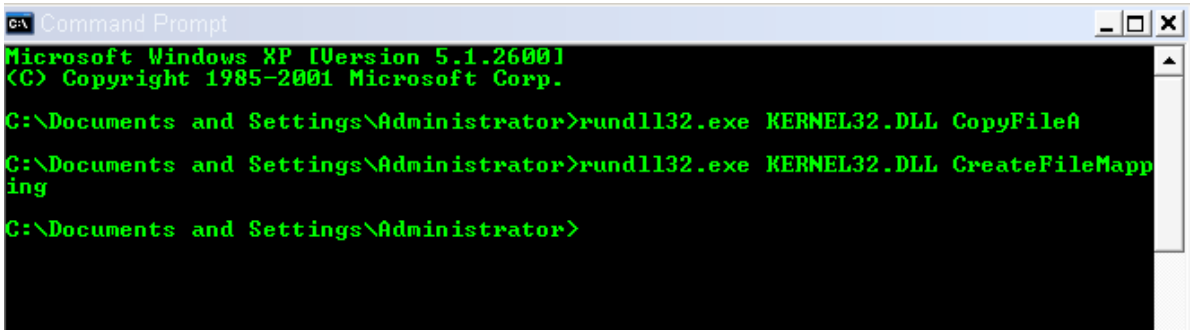

Process Explorer - Sysinternals: www.sysinternals.com [WINSP3UE\Administrator]
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 96.78 0 K 28 K 0
System 0 K 236 K 4
Interrupts < 0.01 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 168 K 388 K 320 Windows NT Session Mana... Microsoft Corporation
csrss.exe 1,596 K 3,308 K 416 Client Server Runtime Process Microsoft Corporation
winlogon.exe 3,552 K 1,752 K 440 Windows NT Logon Applicat... Microsoft Corporation
services.exe 1,600 K 3,268 K 484 Services and Controller app Microsoft Corporation
VBoxService.exe 1,056 K 3,176 K 644 VirtualBox Guest Additions S... Oracle Corporation
lsass.exe 3,696 K 6,016 K 496 LSA Shell (Export Version) Microsoft Corporation
svchost.exe 2,968 K 4,664 K 680 Generic Host Process for Wi... Microsoft Corporation
wmiprvse.exe 2,136 K 4,376 K 1024 WMI Microsoft Corporation
svchost.exe 1,684 K 4,228 K 748 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 10,408 K 15,320 K 784 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,460 K 3,604 K 836 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,436 K 3,864 K 936 Generic Host Process for Wi... Microsoft Corporation
explorer.exe 11,356 K 17,536 K 1104 Windows Explorer Microsoft Corporation
VBoxTray.exe 1,316 K 3,496 K 1676 VirtualBox Guest Additions Tr... Oracle Corporation
vmx32to64.exe 588 K 1,804 K 1684
procexp.exe 3.22 9,772 K 9,128 K 328 Sysinternals Process Explorer Sysinternals - www.sysinter...
spoolsv.exe 2,956 K 4,392 K 1232 Spooler SubSystem App Microsoft Corporation
alg.exe 1,068 K 3,392 K 1548 Application Layer Gateway S... Microsoft Corporation
svchost.exe 860 K 2,208 K 1600 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 860 K 2,204 K 928 Generic Host Process for Wi... Microsoft Corporation
Name Description Company Name Path
user32.dll Windows XP USER API Client DLL Microsoft Corporation C:\WINDOWS\system32\user32.dll
userenv.dll Userenv Microsoft Corporation C:\WINDOWS\system32\userenv.dll
uxtheme.dll Microsoft UxTheme Library Microsoft Corporation C:\WINDOWS\system32\uxtheme.dll
version.dll Version Checking and File Installati... Microsoft Corporation C:\WINDOWS\system32\version.dll
wbemcomn.dll WMI Microsoft Corporation C:\WINDOWS\system32\wbem\wbemcomn.dll
wbemprox.dll WMI Microsoft Corporation C:\WINDOWS\system32\wbem\wbemprox.dll
wbemsvc.dll WMI Microsoft Corporation C:\WINDOWS\system32\wbem\wbemsvc.dll
CPU Usage: 3.22% Commit Charge: 3.67% Processes: 22 Physical Usage: 18.71%
C:\Documents and Se...
Process Explorer - Sy...
8:15 PM

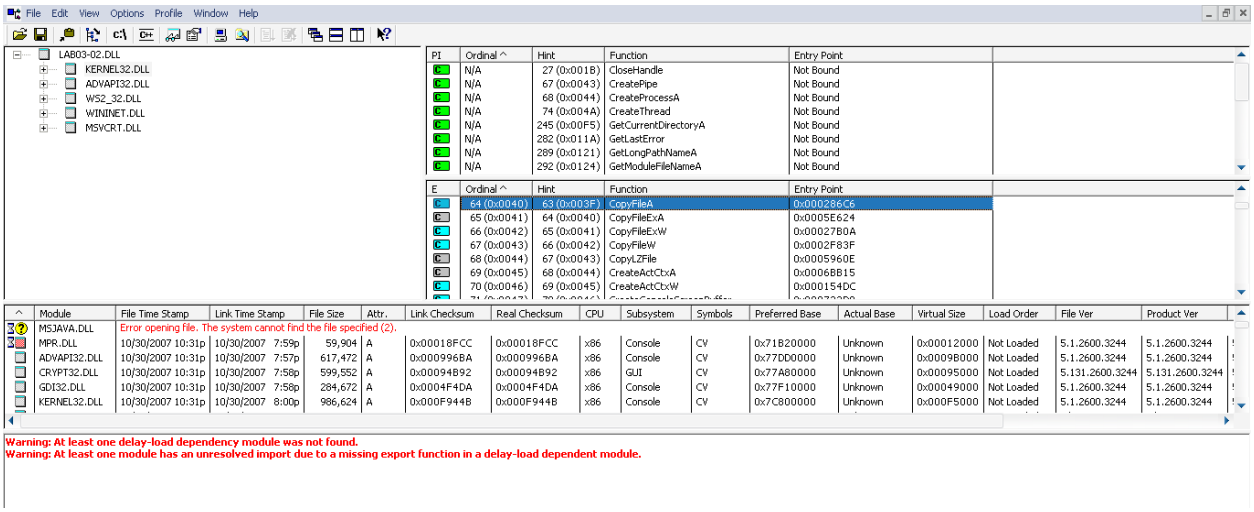

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time... Process Name PID Operation Path Result Detail
7:55:1... Lab03-01.exe 1488 Process Start SUCCESS Parent PID: 1104, ...
7:55:1... Lab03-01.exe 1488 Thread Create SUCCESS Thread ID: 344
7:55:1... Lab03-01.exe 1488 QueryNameInfo... C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Name: \Document...
7:55:1... Lab03-01.exe 1488 Load Image C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Image Base: 0x400...
7:55:1... Lab03-01.exe 1488 Load Image C:\WINDOWS\system32\ntdll.dll SUCCESS Image Base: 0x7c9...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Lab03-01.exe NAME NOT FOUND Desired Access: R...
7:55:1... Lab03-01.exe 1488 CreateFile C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Desired Access: E...
7:55:1... Lab03-01.exe 1488 FileSystemControl C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Control: FSCTL_IS...
7:55:1... Lab03-01.exe 1488 QueryOpen C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... NAME NOT FOUND
7:55:1... Lab03-01.exe 1488 Load Image C:\WINDOWS\system32\kernel32.dll SUCCESS Image Base: 0x7c8...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWO...
7:55:1... Lab03-01.exe 1488 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWO...
7:55:1... Lab03-01.exe 1488 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Desired Access: Q...
7:55:1... Lab03-01.exe 1488 RegQueryValue HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode NAME NOT FOUND Length: 16
7:55:1... Lab03-01.exe 1488 RegCloseKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS
7:55:1... Lab03-01.exe 1488 Load Image C:\WINDOWS\system32\advapi32.dll SUCCESS Image Base: 0x77d...
7:55:1... Lab03-01.exe 1488 Load Image C:\WINDOWS\system32\rpcrt4.dll SUCCESS Image Base: 0x77e...
7:55:1... Lab03-01.exe 1488 Load Image C:\WINDOWS\system32\secur32.dll SUCCESS Image Base: 0x77f...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll NAME NOT FOUND Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll NAME NOT FOUND Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\advapi32.dll NAME NOT FOUND Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWO...
7:55:1... Lab03-01.exe 1488 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled SUCCESS Type: REG_DWO...
7:55:1... Lab03-01.exe 1488 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Desired Access: R...
7:55:1... Lab03-01.exe 1488 RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack NAME NOT FOUND Length: 144
7:55:1... Lab03-01.exe 1488 RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM SUCCESS Desired Access: M...
7:55:1... Lab03-01.exe 1488 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics NAME NOT FOUND Desired Access: R...
Showing 96 of 22,518 events (0.42%) Backed by virtual memory
C:\Documents and Se... Process Monitor - Sys... 7:56 PM


~res-x86_0002 - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2021/12/1 19:20:41 , 2021/12/1 19:21:08
Computer: WINSP3UE , WINSP3UE
Username: Administrator , Administrator
Keys added: 1
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSaveMRU\hiv
Values added: 4
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\LastvisitedMRU\c: 52 00 65 00 67 00 73 00 68 00 6F 00 74 0
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSaveMRU*\c: "C:\Documents and Settings\Administrator\D
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSaveMRU\hiv\a: "C:\Documents and Settings\Administrator
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSaveMRU\hiv\MRUList: "a"
Values modified: 6
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 42 27 24 E7 DF 7B EC B9 48 AF 12 38 8A D3 89 2E FA 20 DF C6 14 03 F8 ED 52 03 FE 81 A4 25 89 DB 13 19 CF F5 9E 99 87 53
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 7D 17 FB AB 4A F1 5E FE F7 5E 39 70 10 92 06 33 23 19 8A D2 F2 B9 83 93 3F 04 92 D0 27 56 88 FB 9F 2C B0 11 E4 E0 63 F9
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\LastvisitedMRU\MRUList: "ba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\LastvisitedMRU\MRUList: "cba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSaveMRU*\MRUList: "ab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\ComDlg32\OpenSaveMRU*\MRUList: "cab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 05 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 04 00 00 00 0
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 05 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 04 00 00 00 0
Total changes: 11
C:\Documents and Se... Regshot 1.9.0 x86 A... ~res-x86_0002 - Not... 8:22 PM

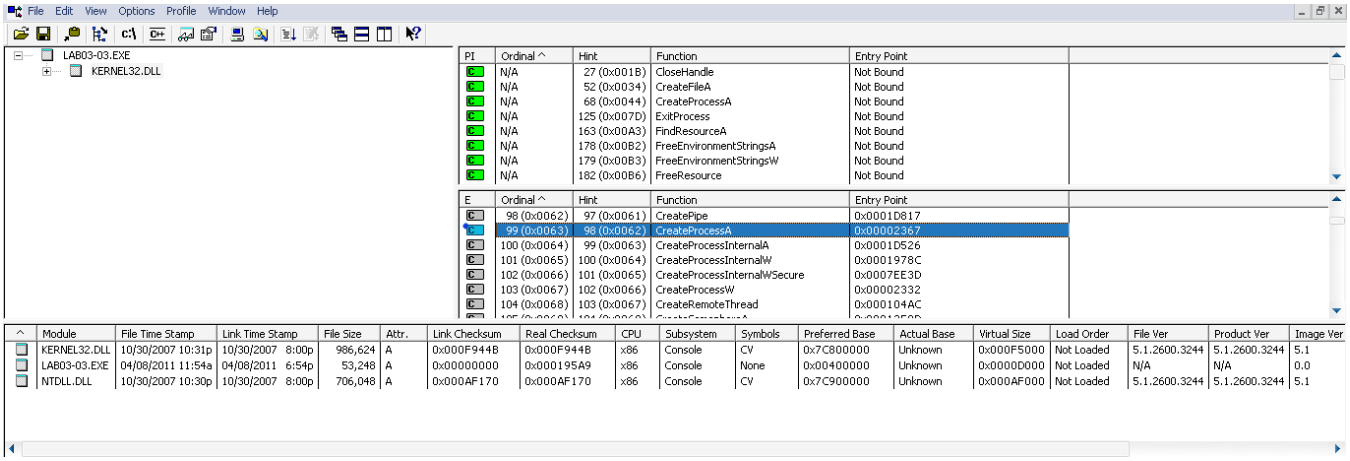
Lab 3-02

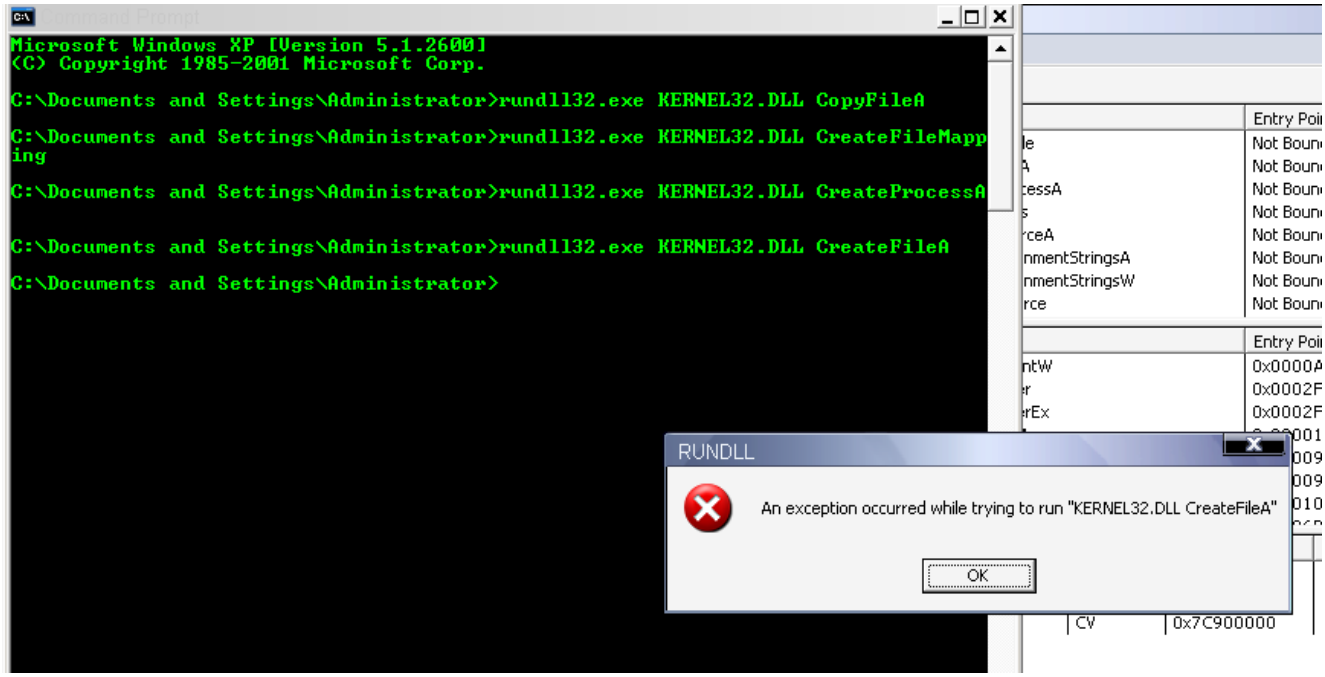

File Edit View Options Profile Window Help
LAB03-02.DLL
KERNEL32.DLL
ADVAPI32.DLL
WS2_32.DLL
WININET.DLL
MSVCRT.DLL
PI Ordinal Hint Function Entry Point
N/A 27 (0x001B) CloseHandle Not Bound
N/A 67 (0x0043) CreatePipe Not Bound
N/A 68 (0x0044) CreateProcessA Not Bound
N/A 74 (0x004A) CreateThread Not Bound
N/A 245 (0x00F5) GetCurrentDirectoryA Not Bound
N/A 282 (0x011A) GetLastError Not Bound
N/A 289 (0x0121) GetLongPathNameA Not Bound
N/A 292 (0x0124) GetModuleFileNameA Not Bound
E Ordinal Hint Function Entry Point
64 (0x0040) 63 (0x003F) CopyFileA 0x000286C6
65 (0x0041) 64 (0x0040) CopyFileExA 0x0005E624
66 (0x0042) 65 (0x0041) CopyFileExW 0x00027B0A
67 (0x0043) 66 (0x0042) CopyFileW 0x0002F83F
68 (0x0044) 67 (0x0043) CopyLZFile 0x0005960E
69 (0x0045) 68 (0x0044) CreateActCtxA 0x0006BB15
70 (0x0046) 69 (0x0045) CreateActCtxW 0x000154DC
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver
MSJAVA.DLL Error opening file. The system cannot find the file specified (2).
MPR.DLL 10/30/2007 10:31p 10/30/2007 7:59p 59,904 A 0x00018FCC 0x00018FCC x86 Console CV 0x71B20000 Unknown 0x00012000 Not Loaded 5.1.2600.3244 5.1.2600.3244
ADVAPI32.DLL 10/30/2007 10:31p 10/30/2007 7:57p 617,472 A 0x000996BA 0x000996BA x86 Console CV 0x77DD0000 Unknown 0x0009B000 Not Loaded 5.1.2600.3244 5.1.2600.3244
CRYPT32.DLL 10/30/2007 10:31p 10/30/2007 7:58p 599,552 A 0x00094B92 0x00094B92 x86 GUI CV 0x77A80000 Unknown 0x00095000 Not Loaded 5.131.2600.3244 5.131.2600.3244
GDI32.DLL 10/30/2007 10:31p 10/30/2007 7:58p 284,672 A 0x0004F4DA 0x0004F4DA x86 Console CV 0x77F10000 Unknown 0x00049000 Not Loaded 5.1.2600.3244 5.1.2600.3244
KERNEL32.DLL 10/30/2007 10:31p 10/30/2007 8:00p 986,624 A 0x000F944B 0x000F944B x86 Console CV 0x7C800000 Unknown 0x000F5000 Not Loaded 5.1.2600.3244 5.1.2600.3244
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

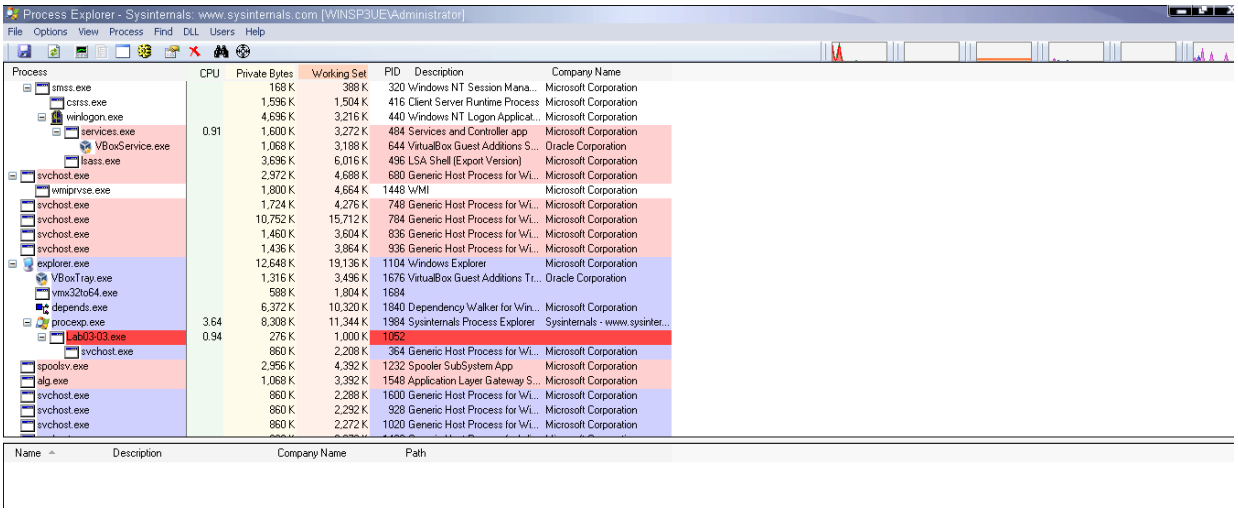

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CopyFileA
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CreateFileMapping
C:\Documents and Settings\Administrator>

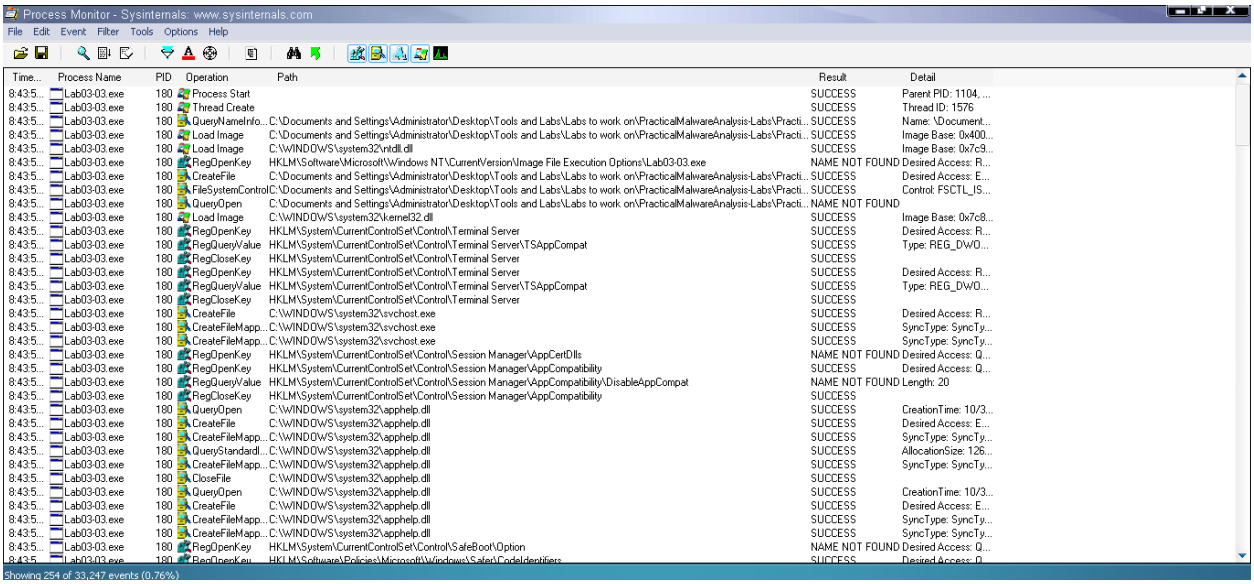

File Edit View Options Profile Window Help
LAB03-02.DLL
KERNEL32.DLL
ADVAPI32.DLL
WS2_32.DLL
WININET.DLL
MSVCRT.DLL
PI Ordinal Hint Function Entry Point
N/A 27 (0x001B) CloseHandle Not Bound
N/A 67 (0x0043) CreatePipe Not Bound
N/A 68 (0x0044) CreateProcessA Not Bound
N/A 74 (0x004A) CreateThread Not Bound
N/A 245 (0x00F5) GetCurrentDirectoryA Not Bound
N/A 282 (0x011A) GetLastError Not Bound
N/A 289 (0x0121) GetLongPathNameA Not Bound
N/A 292 (0x0124) GetModuleFileNameA Not Bound
E Ordinal Hint Function Entry Point
64 (0x0040) 63 (0x003F) CopyFileA 0x000286C6
65 (0x0041) 64 (0x0040) CopyFileExA 0x0005E624
66 (0x0042) 65 (0x0041) CopyFileExW 0x00027B0A
67 (0x0043) 66 (0x0042) CopyFileW 0x0002F83F
68 (0x0044) 67 (0x0043) CopyLZFile 0x0005960E
69 (0x0045) 68 (0x0044) CreateActCtxA 0x0006BB15
70 (0x0046) 69 (0x0045) CreateActCtxW 0x000154DC
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver
MSJAVA.DLL Error opening file. The system cannot find the file specified (2).
MPR.DLL 10/30/2007 10:31p 10/30/2007 7:59p 59,904 A 0x00018FCC 0x00018FCC x86 Console CV 0x71B20000 Unknown 0x00012000 Not Loaded 5.1.2600.3244 5.1.2600.3244
ADVAPI32.DLL 10/30/2007 10:31p 10/30/2007 7:57p 617,472 A 0x000996BA 0x000996BA x86 Console CV 0x77DD0000 Unknown 0x0009B000 Not Loaded 5.1.2600.3244 5.1.2600.3244
CRYPT32.DLL 10/30/2007 10:31p 10/30/2007 7:58p 599,552 A 0x00094B92 0x00094B92 x86 GUI CV 0x77A80000 Unknown 0x00095000 Not Loaded 5.131.2600.3244 5.131.2600.3244
GDI32.DLL 10/30/2007 10:31p 10/30/2007 7:58p 284,672 A 0x0004F4DA 0x0004F4DA x86 Console CV 0x77F10000 Unknown 0x00049000 Not Loaded 5.1.2600.3244 5.1.2600.3244
KERNEL32.DLL 10/30/2007 10:31p 10/30/2007 8:00p 986,624 A 0x000F944B 0x000F944B x86 Console CV 0x7C800000 Unknown 0x000F5000 Not Loaded 5.1.2600.3244 5.1.2600.3244
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

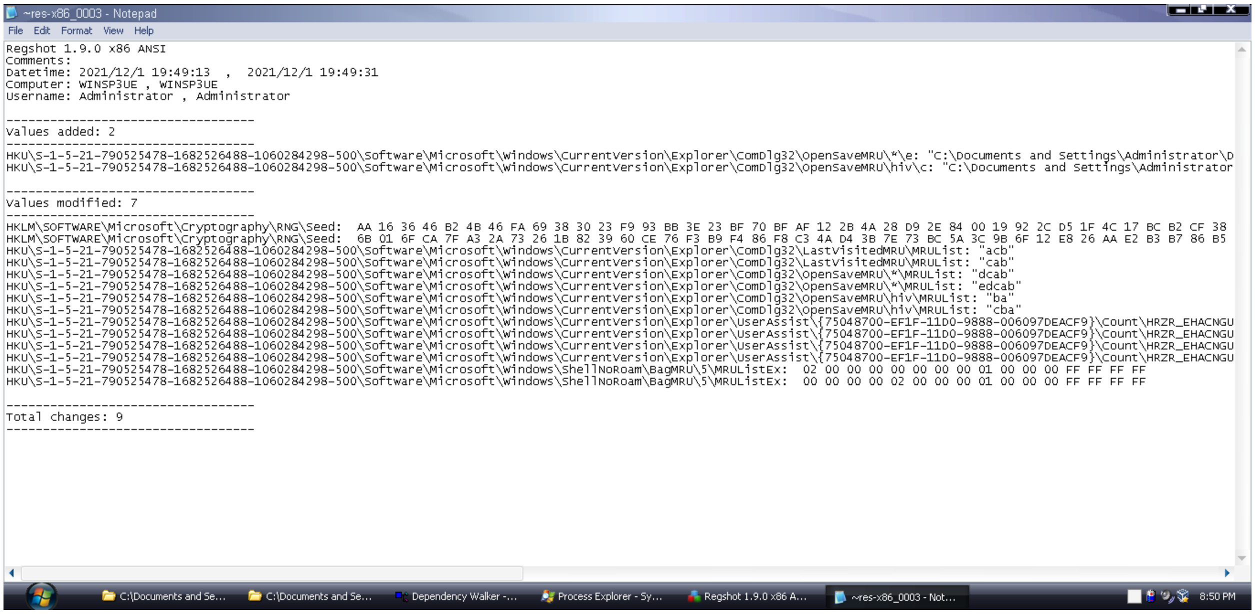
Lab 3-03


File Edit View Options Profile Window Help
LAB03-03.EXE
KERNEL32.DLL
PI Ordinal ^ Hint Function Entry Point
N/A 27 (0x001B) CloseHandle Not Bound
N/A 52 (0x0034) CreateFileA Not Bound
N/A 68 (0x0044) CreateProcessA Not Bound
N/A 125 (0x007D) ExitProcess Not Bound
N/A 163 (0x00A3) FindResourceA Not Bound
N/A 178 (0x00B2) FreeEnvironmentStringsA Not Bound
N/A 179 (0x00B3) FreeEnvironmentStringsW Not Bound
N/A 182 (0x00B6) FreeResource Not Bound
E Ordinal ^ Hint Function Entry Point
98 (0x0062) 97 (0x0061) CreatePipe 0x0001D817
99 (0x0063) 98 (0x0062) CreateProcessA 0x00002367
100 (0x0064) 99 (0x0063) CreateProcessInternalA 0x0001D526
101 (0x0065) 100 (0x0064) CreateProcessInternalW 0x0001978C
102 (0x0066) 101 (0x0065) CreateProcessInternalWSecure 0x0007EE3D
103 (0x0067) 102 (0x0066) CreateProcessW 0x00002332
104 (0x0068) 103 (0x0067) CreateRemoteThread 0x000104AC
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver Image Ver
KERNEL32.DLL 10/30/2007 10:31p 10/30/2007 8:00p 986,624 A 0x000F944B 0x000F944B x86 Console CV 0x7C800000 Unknown 0x000F5000 Not Loaded 5.1.2600.3244 5.1.2600.3244 5.1
LAB03-03.EXE 04/08/2011 11:54a 04/08/2011 6:54p 53,248 A 0x00000000 0x000195A9 x86 Console None 0x00400000 Unknown 0x0000D000 Not Loaded N/A N/A 0.0
NTDLL.DLL 10/30/2007 10:30p 10/30/2007 8:00p 706,048 A 0x000AF170 0x000AF170 x86 Console CV 0x7C900000 Unknown 0x000AF000 Not Loaded 5.1.2600.3244 5.1.2600.3244 5.1


Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CopyFileA
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CreateFileMapping
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CreateProcessA
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL CreateFileA
C:\Documents and Settings\Administrator>
RUNDLL
An exception occurred while trying to run "KERNEL32.DLL CreateFileA"
OK
CV
0x7C900000

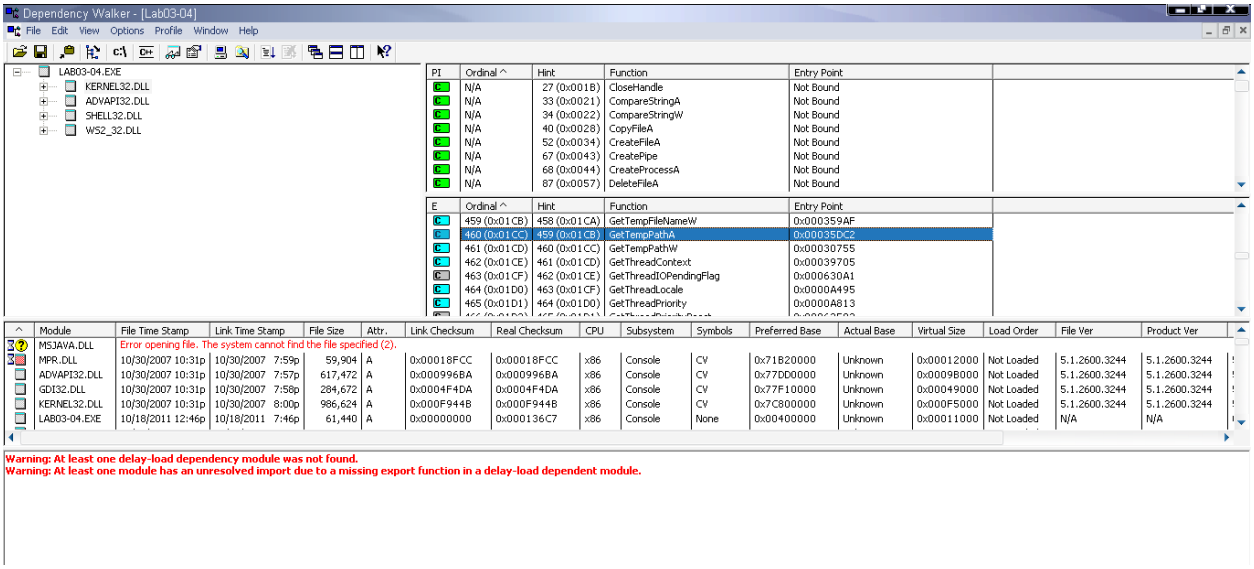

Process Explorer - Sysinternals: www.sysinternals.com [WINSP3UE\Administrator]
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set PID Description Company Name
smss.exe 168 K 388 K 320 Windows NT Session Mana... Microsoft Corporation
csrss.exe 1,596 K 1,504 K 416 Client Server Runtime Process Microsoft Corporation
winlogon.exe 4,696 K 3,216 K 440 Windows NT Logon Applicat... Microsoft Corporation
services.exe 0.91 1,600 K 3,272 K 484 Services and Controller app Microsoft Corporation
VBoxService.exe 1,068 K 3,188 K 644 VirtualBox Guest Additions S... Oracle Corporation
lsass.exe 3,696 K 6,016 K 496 LSA Shell (Export Version) Microsoft Corporation
svchost.exe 2,972 K 4,688 K 680 Generic Host Process for Wi... Microsoft Corporation
wmiprvse.exe 1,800 K 4,664 K 1448 WMI Microsoft Corporation
svchost.exe 1,724 K 4,276 K 748 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 10,752 K 15,712 K 784 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,460 K 3,604 K 836 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,436 K 3,864 K 936 Generic Host Process for Wi... Microsoft Corporation
explorer.exe 12,648 K 19,136 K 1104 Windows Explorer Microsoft Corporation
VBoxTray.exe 1,316 K 3,496 K 1676 VirtualBox Guest Additions Tr... Oracle Corporation
vmx32to64.exe 588 K 1,804 K 1684
depends.exe 6,372 K 10,320 K 1840 Dependency Walker for Win... Microsoft Corporation
procexp.exe 3.64 8,308 K 11,344 K 1984 Sysinternals Process Explorer Sysinternals - www.sysinter...
Lab03-03.exe 0.94 276 K 1,000 K 1052
svchost.exe 860 K 2,208 K 364 Generic Host Process for Wi... Microsoft Corporation
spoolsv.exe 2,956 K 4,392 K 1232 Spooler SubSystem App Microsoft Corporation
alg.exe 1,068 K 3,392 K 1548 Application Layer Gateway S... Microsoft Corporation
svchost.exe 860 K 2,288 K 1600 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 860 K 2,292 K 928 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 860 K 2,272 K 1020 Generic Host Process for Wi... Microsoft Corporation
Name Description Company Name Path

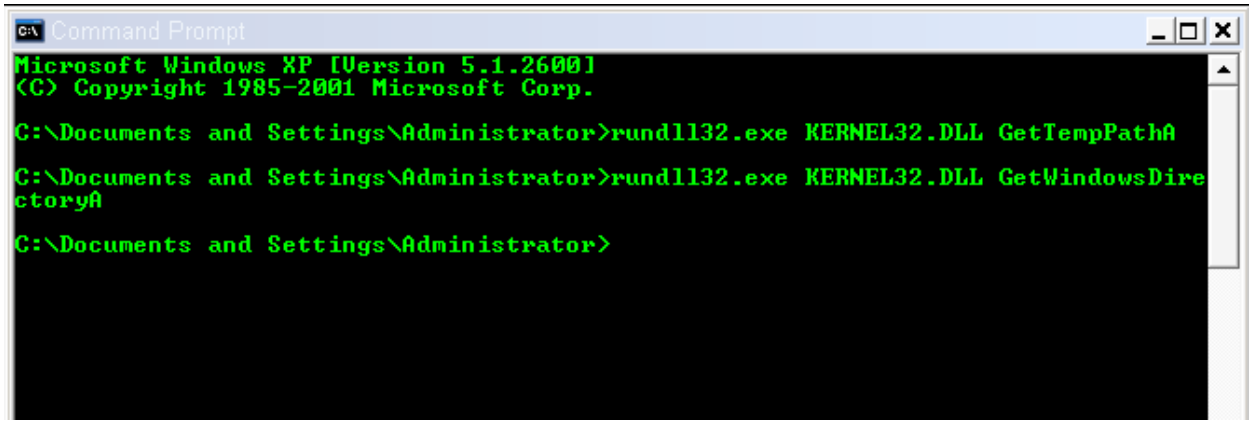

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time... Process Name PID Operation Path Result Detail
8:43:5... Lab03-03.exe 180 Process Start SUCCESS Parent PID: 1104, ...
8:43:5... Lab03-03.exe 180 Thread Create SUCCESS Thread ID: 1576
8:43:5... Lab03-03.exe 180 QueryNameInfo... C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Name: \Document...
8:43:5... Lab03-03.exe 180 Load Image C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Image Base: 0x400...
8:43:5... Lab03-03.exe 180 Load Image C:\WINDOWS\system32\ntdll.dll SUCCESS Image Base: 0x7c9...
8:43:5... Lab03-03.exe 180 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Lab03-03.exe NAME NOT FOUND Desired Access: R...
8:43:5... Lab03-03.exe 180 CreateFile C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Desired Access: E...
8:43:5... Lab03-03.exe 180 FileSystemControl C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... SUCCESS Control: FSCTL_IS...
8:43:5... Lab03-03.exe 180 QueryOpen C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi... NAME NOT FOUND
8:43:5... Lab03-03.exe 180 Load Image C:\WINDOWS\system32\kernel32.dll SUCCESS Image Base: 0x7c8...
8:43:5... Lab03-03.exe 180 RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: R...
8:43:5... Lab03-03.exe 180 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWO...
8:43:5... Lab03-03.exe 180 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
8:43:5... Lab03-03.exe 180 RegOpenKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS Desired Access: R...
8:43:5... Lab03-03.exe 180 RegQueryValue HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat SUCCESS Type: REG_DWO...
8:43:5... Lab03-03.exe 180 RegCloseKey HKLM\System\CurrentControlSet\Control\Terminal Server SUCCESS
8:43:5... Lab03-03.exe 180 CreateFile C:\WINDOWS\system32\svchost.exe SUCCESS Desired Access: R...
8:43:5... Lab03-03.exe 180 CreateFileMapp... C:\WINDOWS\system32\svchost.exe SUCCESS SyncType: SyncTy...
8:43:5... Lab03-03.exe 180 CreateFileMapp... C:\WINDOWS\system32\svchost.exe SUCCESS SyncType: SyncTy...
8:43:5... Lab03-03.exe 180 RegOpenKey HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls NAME NOT FOUND Desired Access: Q...
8:43:5... Lab03-03.exe 180 RegOpenKey HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility SUCCESS Desired Access: Q...
8:43:5... Lab03-03.exe 180 RegQueryValue HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\DisableAppCompat NAME NOT FOUND Length: 20
8:43:5... Lab03-03.exe 180 RegCloseKey HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility SUCCESS
8:43:5... Lab03-03.exe 180 QueryOpen C:\WINDOWS\system32\apphelp.dll SUCCESS CreationTime: 10/3...
8:43:5... Lab03-03.exe 180 CreateFile C:\WINDOWS\system32\apphelp.dll SUCCESS Desired Access: E...
8:43:5... Lab03-03.exe 180 CreateFileMapp... C:\WINDOWS\system32\apphelp.dll SUCCESS SyncType: SyncTy...
8:43:5... Lab03-03.exe 180 QueryStandardI... C:\WINDOWS\system32\apphelp.dll SUCCESS AllocationSize: 126...
8:43:5... Lab03-03.exe 180 CreateFileMapp... C:\WINDOWS\system32\apphelp.dll SUCCESS SyncType: SyncTy...
8:43:5... Lab03-03.exe 180 CloseFile C:\WINDOWS\system32\apphelp.dll SUCCESS
8:43:5... Lab03-03.exe 180 QueryOpen C:\WINDOWS\system32\apphelp.dll SUCCESS CreationTime: 10/3...
8:43:5... Lab03-03.exe 180 CreateFile C:\WINDOWS\system32\apphelp.dll SUCCESS Desired Access: E...
8:43:5... Lab03-03.exe 180 CreateFileMapp... C:\WINDOWS\system32\apphelp.dll SUCCESS SyncType: SyncTy...
8:43:5... Lab03-03.exe 180 CreateFileMapp... C:\WINDOWS\system32\apphelp.dll SUCCESS SyncType: SyncTy...
8:43:5... Lab03-03.exe 180 RegOpenKey HKLM\System\CurrentControlSet\Control\SafeBoot\Option NAME NOT FOUND Desired Access: Q...
Showing 254 of 33,247 events (0.76%)

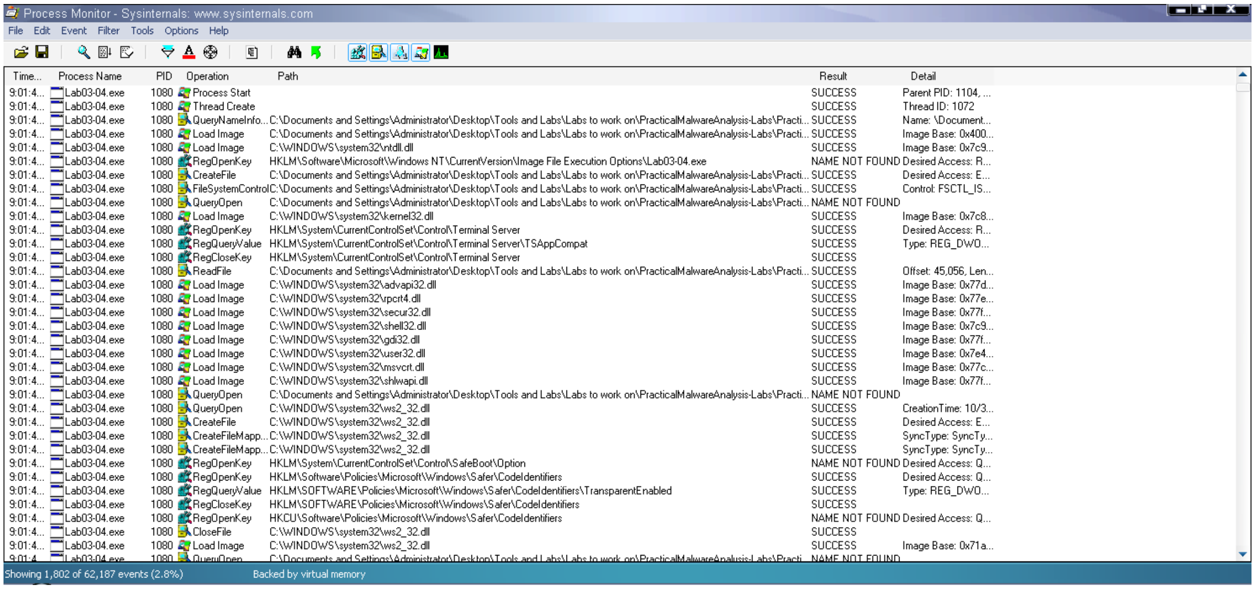



```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2021/12/1 19:49:13  ,  2021/12/1 19:49:31
Computer: WINSP3UE , WINSP3UE
Username: Administrator , Administrator

----------------------------------
Values added: 2
----------------------------------
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\e: "C:\Documents and Settings\Administrator\D
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\c: "C:\Documents and Settings\Administrator

----------------------------------
Values modified: 7
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  AA 16 36 46 B2 4B 46 FA 69 38 30 23 F9 93 BB 3E 23 BF 70 BF AF 12 2B 4A 28 D9 2E 84 00 19 92 2C D5 1F 4C 17 BC B2 CF 38
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  6B 01 6F CA 7F A3 2A 73 26 1B 82 39 60 CE 76 F3 B9 F4 86 F8 C3 4A D4 3B 7E 73 BC 5A 3C 9B 6F 12 E8 26 AA E2 B3 B7 86 B5
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList: "acb"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList: "cab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "dcab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "edcab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\MRUList: "ba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\MRUList: "cba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\MRUListEx:  02 00 00 00 00 00 00 00 01 00 00 00 FF FF FF FF
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\MRUListEx:  00 00 00 00 02 00 00 00 01 00 00 00 FF FF FF FF

----------------------------------
Total changes: 9
----------------------------------
```

Lab 3-04


Dependency Walker - [Lab03-04]
File Edit View Options Profile Window Help
LAB03-04.EXE
KERNEL32.DLL
ADVAPI32.DLL
SHELL32.DLL
WS2_32.DLL
PI Ordinal Hint Function Entry Point
N/A 27 (0x001B) CloseHandle Not Bound
N/A 33 (0x0021) CompareStringA Not Bound
N/A 34 (0x0022) CompareStringW Not Bound
N/A 40 (0x0028) CopyFileA Not Bound
N/A 52 (0x0034) CreateFileA Not Bound
N/A 67 (0x0043) CreatePipe Not Bound
N/A 68 (0x0044) CreateProcessA Not Bound
N/A 87 (0x0057) DeleteFileA Not Bound
E Ordinal Hint Function Entry Point
459 (0x01CB) 458 (0x01CA) GetTempFileNameW 0x000359AF
460 (0x01CC) 459 (0x01CB) GetTempPathA 0x00035DC2
461 (0x01CD) 460 (0x01CC) GetTempPathW 0x00030755
462 (0x01CE) 461 (0x01CD) GetThreadContext 0x00039705
463 (0x01CF) 462 (0x01CE) GetThreadIOPendingFlag 0x000630A1
464 (0x01D0) 463 (0x01CF) GetThreadLocale 0x0000A495
465 (0x01D1) 464 (0x01D0) GetThreadPriority 0x0000A813
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size Load Order File Ver Product Ver
MSJAVA.DLL Error opening file. The system cannot find the file specified (2).
MPR.DLL 10/30/2007 10:31p 10/30/2007 7:59p 59,904 A 0x00018FCC 0x00018FCC x86 Console CV 0x71B20000 Unknown 0x00012000 Not Loaded 5.1.2600.3244 5.1.2600.3244
ADVAPI32.DLL 10/30/2007 10:31p 10/30/2007 7:57p 617,472 A 0x000996BA 0x000996BA x86 Console CV 0x77DD0000 Unknown 0x0009B000 Not Loaded 5.1.2600.3244 5.1.2600.3244
GDI32.DLL 10/30/2007 10:31p 10/30/2007 7:58p 284,672 A 0x0004F4DA 0x0004F4DA x86 Console CV 0x77F10000 Unknown 0x00049000 Not Loaded 5.1.2600.3244 5.1.2600.3244
KERNEL32.DLL 10/30/2007 10:31p 10/30/2007 8:00p 986,624 A 0x000F944B 0x000F944B x86 Console CV 0x7C800000 Unknown 0x000F5000 Not Loaded 5.1.2600.3244 5.1.2600.3244
LAB03-04.EXE 10/18/2011 12:46p 10/18/2011 7:46p 61,440 A 0x00000000 0x000136C7 x86 Console None 0x00400000 Unknown 0x00011000 Not Loaded N/A N/A
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.


Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL GetTempPathA
C:\Documents and Settings\Administrator>rundll32.exe KERNEL32.DLL GetWindowsDire
ctoryA
C:\Documents and Settings\Administrator>

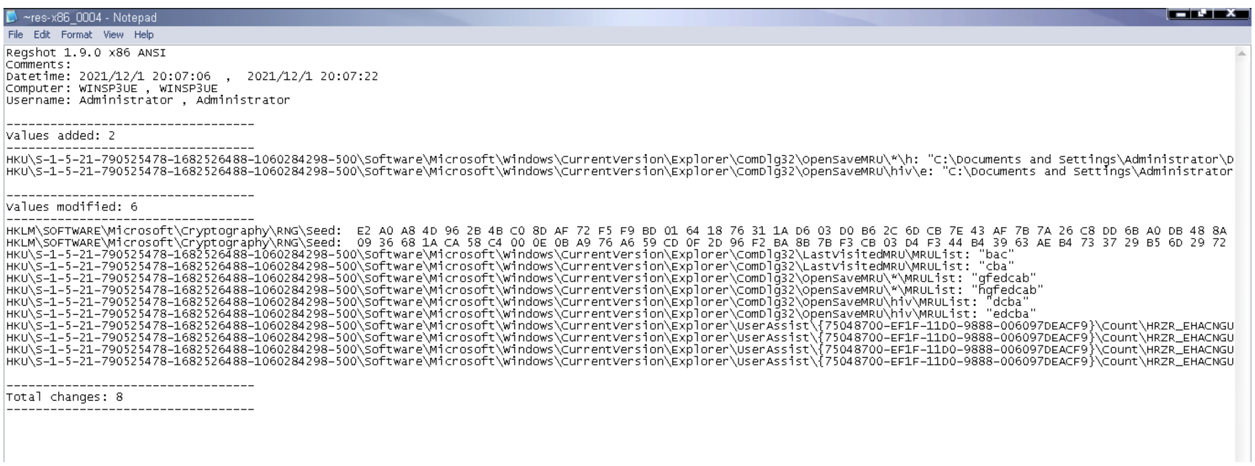


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
9:01:4...	Lab03-04.exe	1080	Process Start		SUCCESS	Parent PID: 1104, ...
9:01:4...	Lab03-04.exe	1080	Thread Create		SUCCESS	Thread ID: 1072
9:01:4...	Lab03-04.exe	1080	QueryNameInfo...	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	SUCCESS	Name: \Document...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	SUCCESS	Image Base: 0x400...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
9:01:4...	Lab03-04.exe	1080	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Lab03-04.exe	NAME NOT FOUND	Desired Access: R...
9:01:4...	Lab03-04.exe	1080	CreateFile	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	SUCCESS	Desired Access: E...
9:01:4...	Lab03-04.exe	1080	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	SUCCESS	Control: FSCTL_IS...
9:01:4...	Lab03-04.exe	1080	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	NAME NOT FOUND	
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
9:01:4...	Lab03-04.exe	1080	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
9:01:4...	Lab03-04.exe	1080	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
9:01:4...	Lab03-04.exe	1080	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
9:01:4...	Lab03-04.exe	1080	ReadFile	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	SUCCESS	Offset: 45,056, Len...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c9...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f...
9:01:4...	Lab03-04.exe	1080	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	NAME NOT FOUND	
9:01:4...	Lab03-04.exe	1080	QueryOpen	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	CreationTime: 10/3...
9:01:4...	Lab03-04.exe	1080	CreateFile	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	Desired Access: E...
9:01:4...	Lab03-04.exe	1080	CreateFileMapp...	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	SyncType: SyncTy...
9:01:4...	Lab03-04.exe	1080	CreateFileMapp...	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	SyncType: SyncTy...
9:01:4...	Lab03-04.exe	1080	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Q...
9:01:4...	Lab03-04.exe	1080	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Q...
9:01:4...	Lab03-04.exe	1080	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	SUCCESS	Type: REG_DWO...
9:01:4...	Lab03-04.exe	1080	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
9:01:4...	Lab03-04.exe	1080	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Q...
9:01:4...	Lab03-04.exe	1080	CloseFile	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	
9:01:4...	Lab03-04.exe	1080	Load Image	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	Image Base: 0x71a...
9:01:4...	Lab03-04.exe	1080	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Tools and Labs\Labs to work on\PracticalMalwareAnalysis-Labs\Practi...	NAME NOT FOUND	

Showing 1,802 of 62,187 events (2.8%) Backed by virtual memory



~res-x86_0004 - Notepad

File Edit Format View Help

```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2021/12/1 20:07:06  ,  2021/12/1 20:07:22
Computer: WINSP3UE , WINSP3UE
Username: Administrator , Administrator

----------------------------------
Values added: 2
----------------------------------
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\h: "C:\Documents and Settings\Administrator\D
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\e: "C:\Documents and Settings\Administrator

----------------------------------
Values modified: 6
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  E2 A0 A8 4D 96 2B 4B C0 8D AF 72 F5 F9 BD 01 64 18 76 31 1A D6 03 D0 B6 2C 6D CB 7E 43 AF 7B 7A 26 C8 DD 6B A0 DB 48 8A
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  09 36 68 1A CA 58 C4 00 0E 0B A9 76 A6 59 CD 0F 2D 96 F2 BA 8B 7B F3 CB 03 D4 F3 44 B4 39 63 AE B4 73 37 29 B5 6D 29 72
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList: "bac"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList: "cba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "gfedcab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "hgfedcab"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\MRUList: "dcba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\MRUList: "edcba"
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU
HKU\S-1-5-21-790525478-1682526488-1060284298-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU

----------------------------------
Total changes: 8
----------------------------------
```