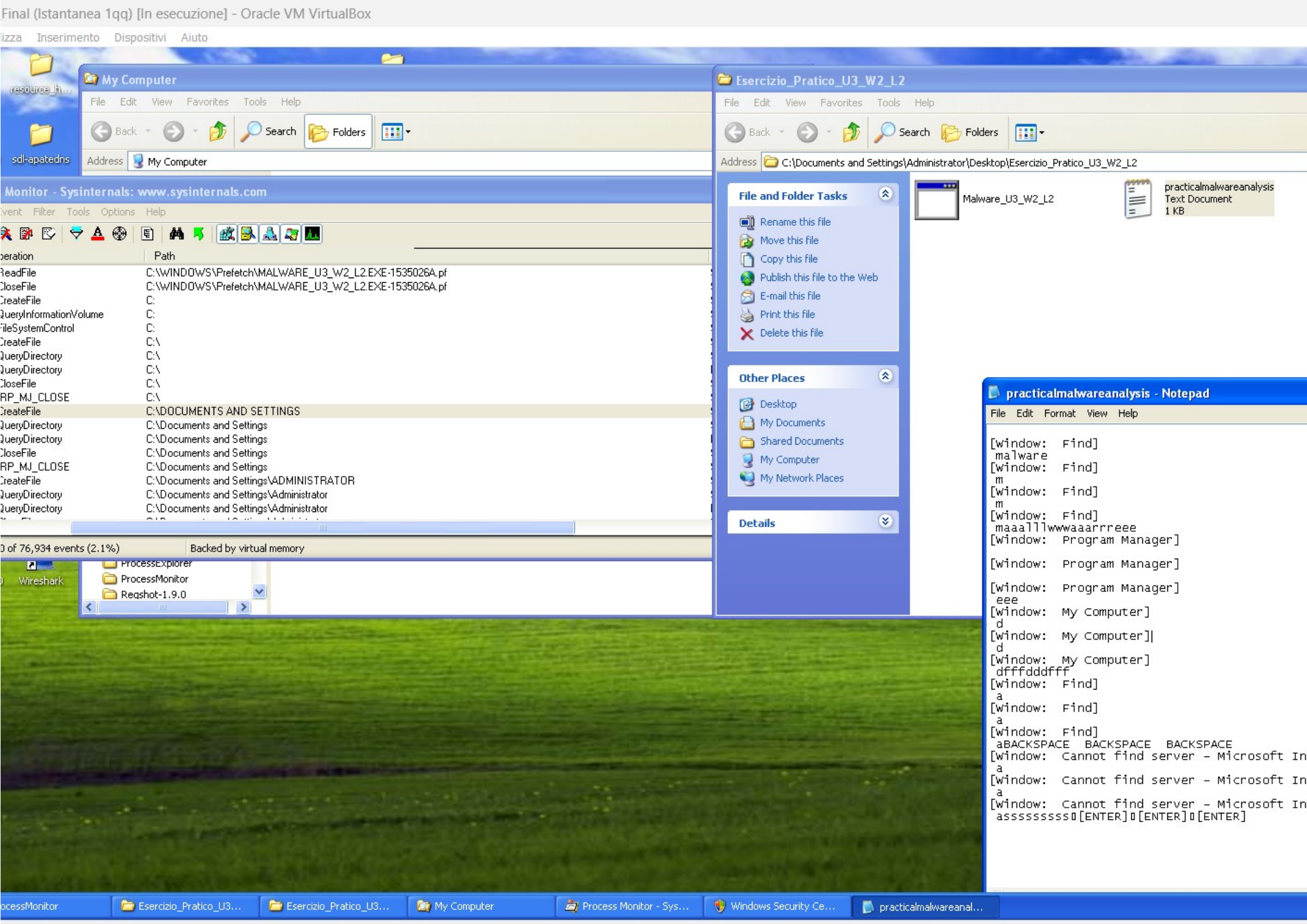
Final (Istantanea 1qq) [In esecuzione] - Oracle VM VirtualBox
Inserimento Dispositivi Aiuto
My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Monitor - Sysinternals: www.sysinternals.com
Vent Filter Tools Options Help
Operation Path
ReadFile C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
CloseFile C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
CreateFile C:
QueryInformationVolume C:
FileSystemControl C:
CreateFile C:\
QueryDirectory C:\
QueryDirectory C:\
CloseFile C:\
IRP_MJ_CLOSE C:\
CreateFile C:\DOCUMENTS AND SETTINGS
QueryDirectory C:\Documents and Settings
QueryDirectory C:\Documents and Settings
CloseFile C:\Documents and Settings
IRP_MJ_CLOSE C:\Documents and Settings
CreateFile C:\Documents and Settings\ADMINISTRATOR
QueryDirectory C:\Documents and Settings\Administrator
QueryDirectory C:\Documents and Settings\Administrator
of 76,934 events (2.1%)
Backed by virtual memory
Wireshark
ProcessExplorer
ProcessMonitor
Regshot-1.9.0
Esercizio_Pratico_U3_W2_L2
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Print this file
Delete this file
Other Places
Desktop
My Documents
Shared Documents
My Computer
My Network Places
Details
Malware_U3_W2_L2
practicalmalwareanalysis
Text Document
1 KB
practicalmalwareanalysis - Notepad
File Edit Format View Help
[window: Find]
malware
[window: Find]
m
[window: Find]
m
[window: Find]
maaalllwwwaaarrreee
[window: Program Manager]
[window: Program Manager]
[window: Program Manager]
eee
[window: My Computer]
d
[window: My Computer]
d
[window: My Computer]
dfffdddfff
[window: Find]
a
[window: Find]
a
[window: Find]
aBACKSPACE BACKSPACE BACKSPACE
[window: Cannot find server - Microsoft In
a
[window: Cannot find server - Microsoft In
a
[window: Cannot find server - Microsoft In
asssssssss[ENTER][ENTER][ENTER]
ocessMonitor
Esercizio_Pratico_U3...
Esercizio_Pratico_U3...
My Computer
Process Monitor - Sys...
Windows Security Ce...
practicalmalwareanal...