Pratica W21D4

Traccia:

EPICODE

Esercizio
Analisi statica e dinamica

Traccia:

Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto.
Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC.
Il file "sospetto" è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer (no, non ridete ragazzi)

Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno.

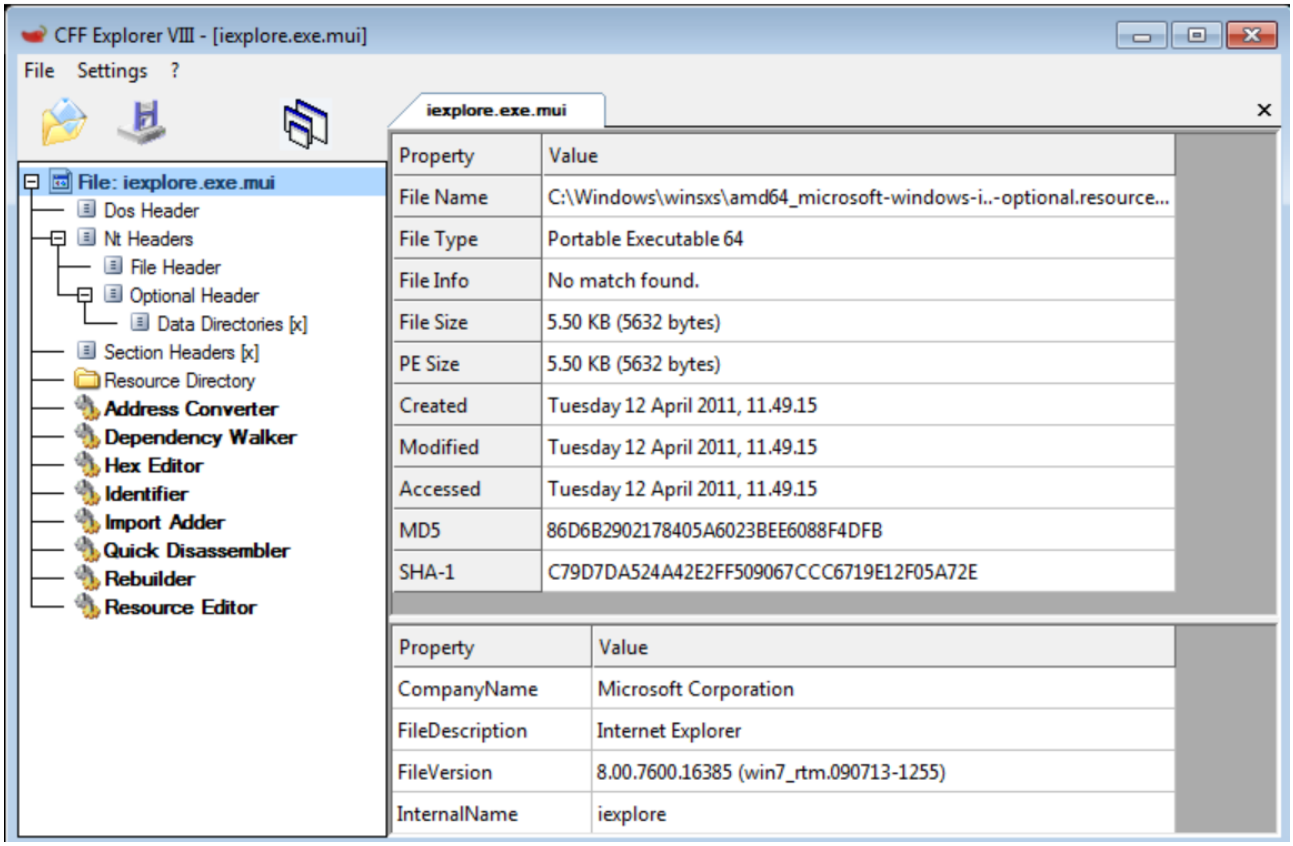
Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione.
No disassembly no debug o similari

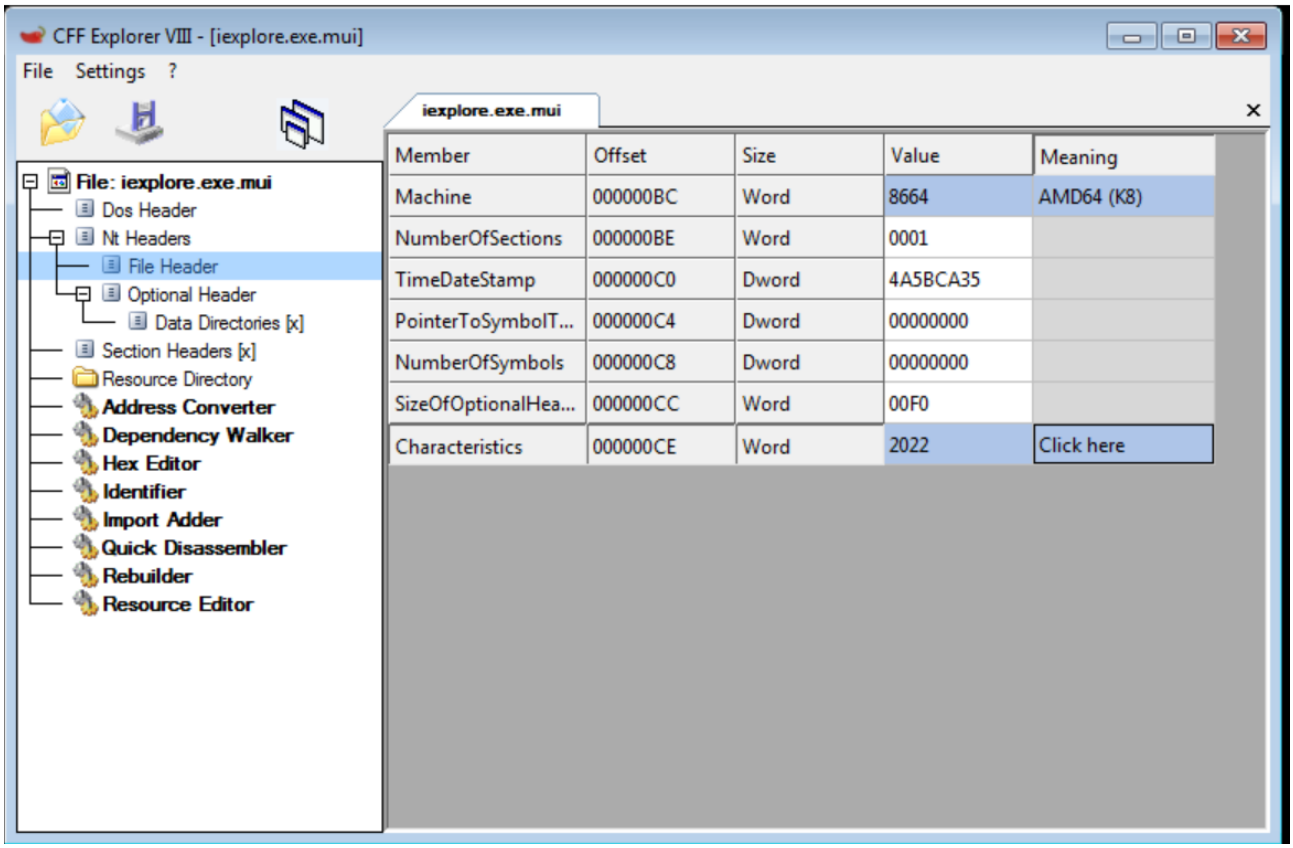
VirusTotal non basta, ovviamente
Non basta dire iexplorer è Microsoft è buono, punto.

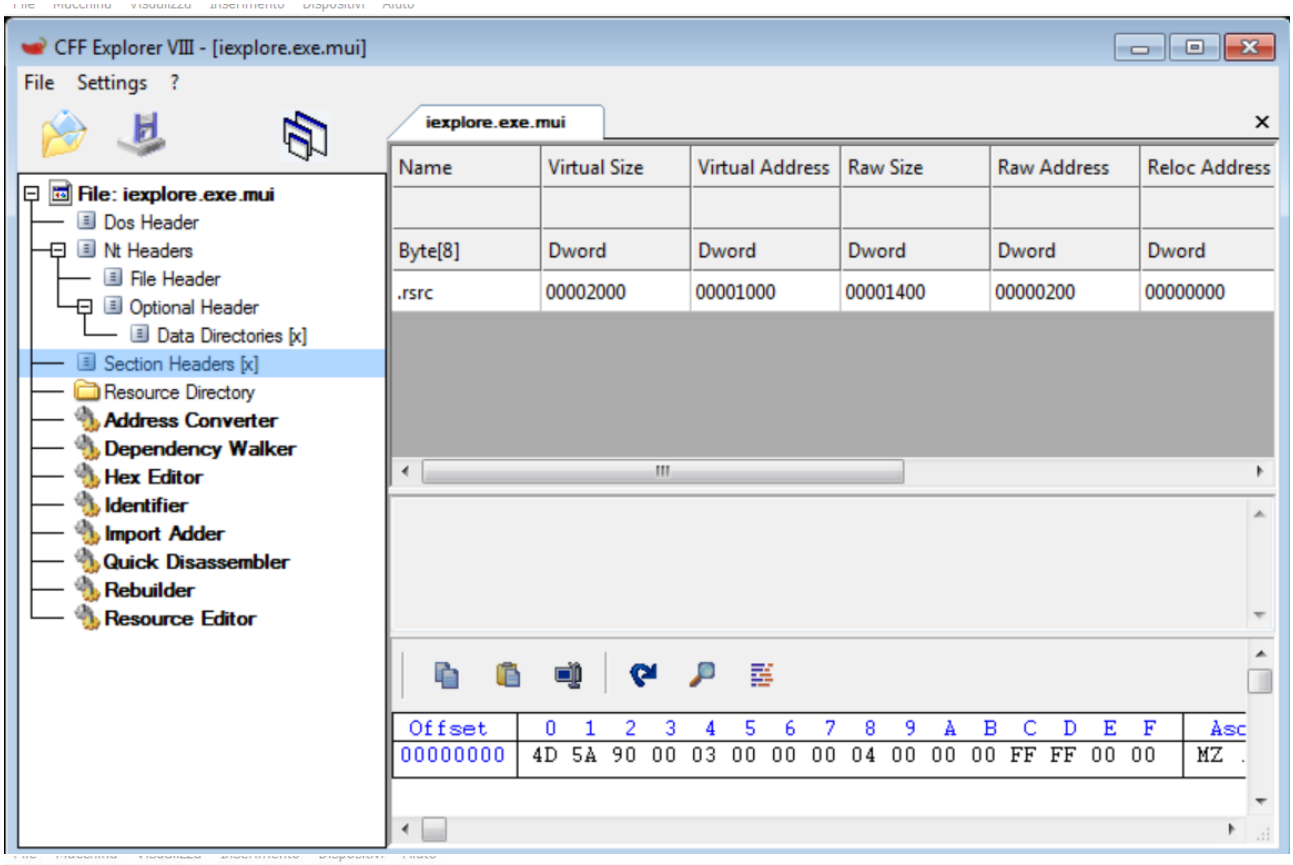
Soluzione:

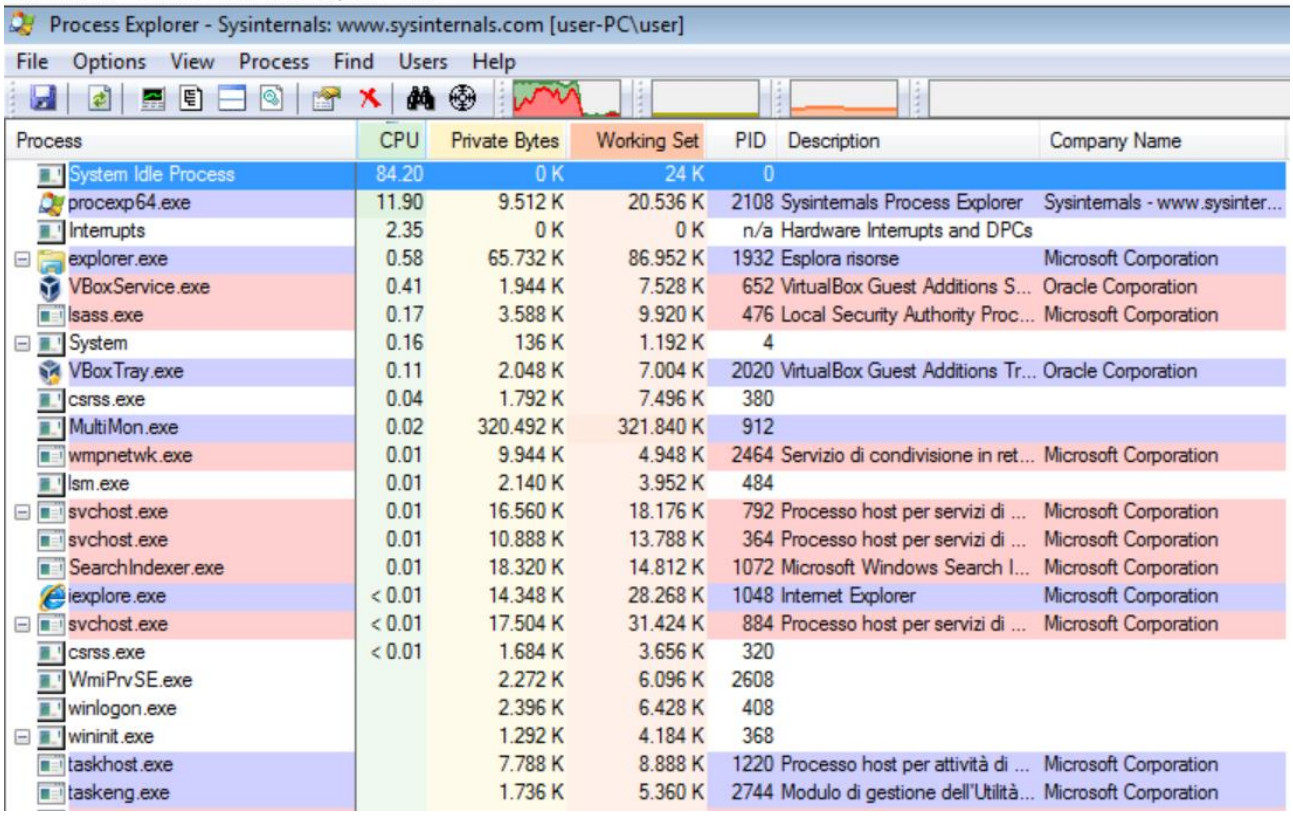
Analizziamo il file IEXPLORE.EXE per valutare la presenza di eventuali azioni sospette. Andiamo ad utilizzare i vari tool utilizzati per l'esercizio precedente, in aggiunta utilizziamo anche il tool **Resource Hacker,** questo è uno strumento di modifica delle risorse per il sistema operativo Windows. È progettato per consentire agli utenti di visualizzare, modificare, aggiungere, ebra o estrarre le risorse incorporate all'interno dei file eseguibili (come .exe, .dll, .ocx, .cpl) e dei file di risorse (come .res o .rc). Queste risorse possono includere icone, immagini, stringhe di testo, cursori, manifesti delle applicazioni e altro ancora.

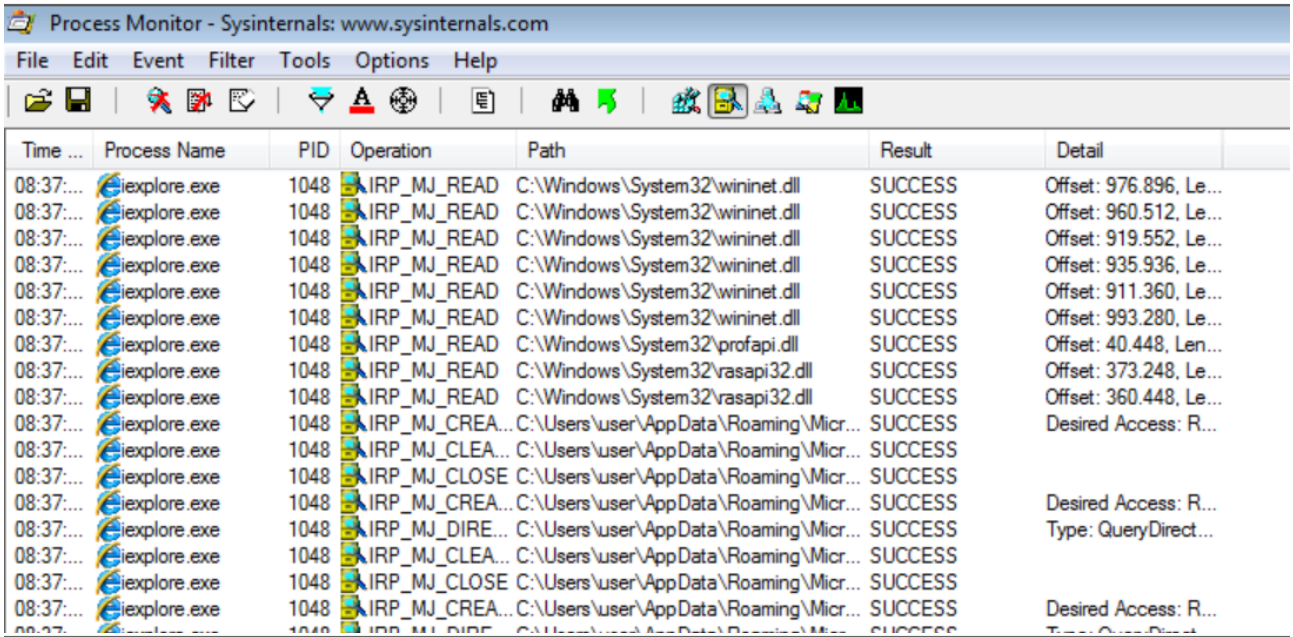
NON SONO STATE RILEVATE ATTIVITà SOSPETTE.

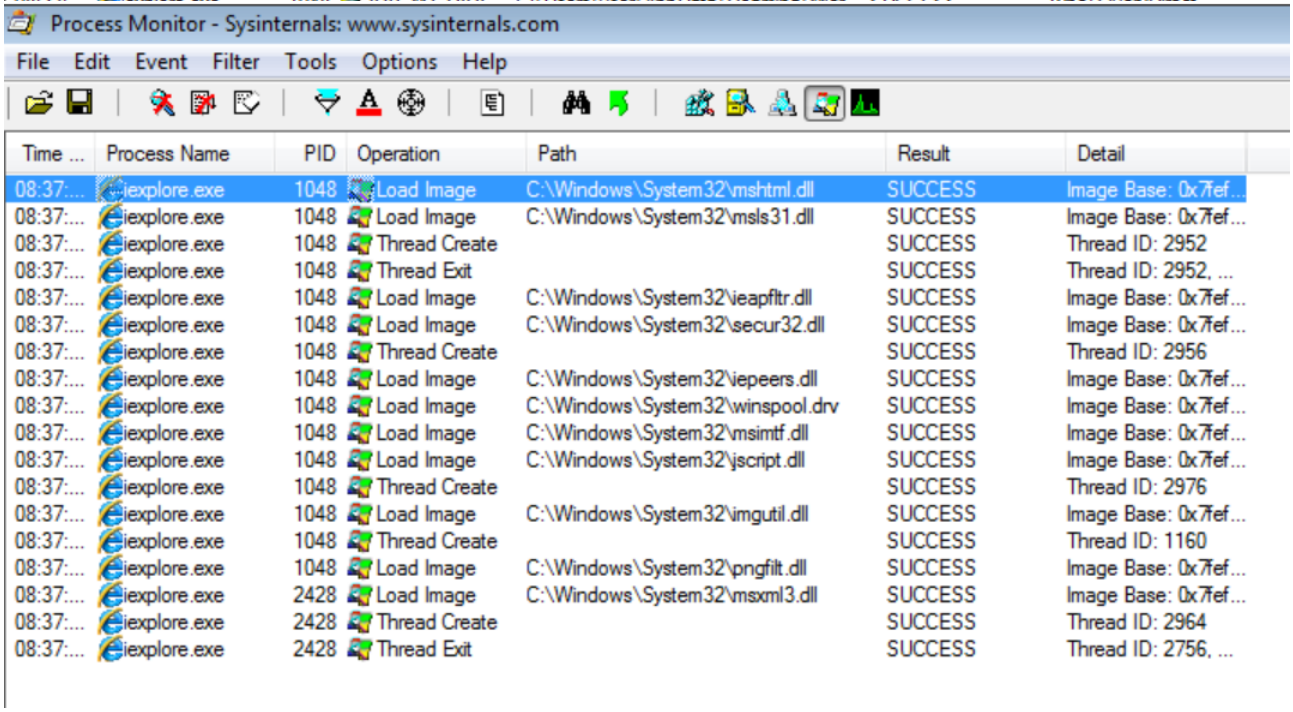

CFF Explorer VIII - [iexplore.exe.mui]
File Settings ?
File: iexplore.exe.mui
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
iexplore.exe.mui
Property Value
File Name C:\Windows\winsxs\amd64_microsoft-windows-i..-optional.resource...
File Type Portable Executable 64
File Info No match found.
File Size 5.50 KB (5632 bytes)
PE Size 5.50 KB (5632 bytes)
Created Tuesday 12 April 2011, 11.49.15
Modified Tuesday 12 April 2011, 11.49.15
Accessed Tuesday 12 April 2011, 11.49.15
MD5 86D6B2902178405A6023BEE6088F4DFB
SHA-1 C79D7DA524A42E2FF509067CCC6719E12F05A72E
Property Value
CompanyName Microsoft Corporation
FileDescription Internet Explorer
FileVersion 8.00.7600.16385 (win7_rtm.090713-1255)
InternalName iexplore

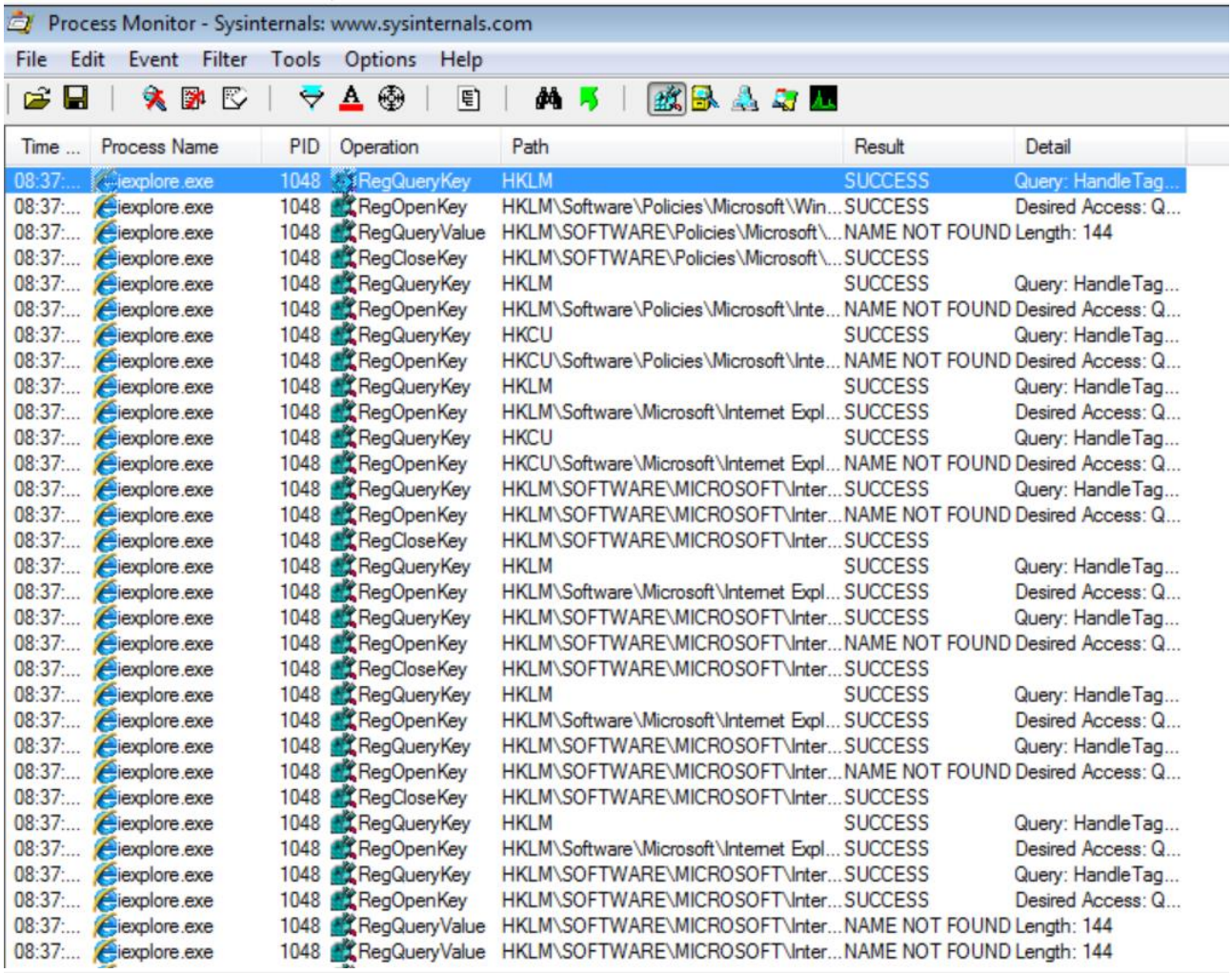

CFF Explorer VIII - [iexplore.exe.mui]
File Settings ?
File: iexplore.exe.mui
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
iexplore.exe.mui
Member Offset Size Value Meaning
Machine 000000BC Word 8664 AMD64 (K8)
NumberOfSections 000000BE Word 0001
TimeDateStamp 000000C0 Dword 4A5BCA35
PointerToSymbolT... 000000C4 Dword 00000000
NumberOfSymbols 000000C8 Dword 00000000
SizeOfOptionalHea... 000000CC Word 00F0
Characteristics 000000CE Word 2022 Click here


CFF Explorer VIII - [iexplore.exe.mui]
File Settings ?
iexplore.exe.mui
File: iexplore.exe.mui
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
Name Virtual Size Virtual Address Raw Size Raw Address Reloc Address
Byte[8] Dword Dword Dword Dword Dword
.rsrc 00002000 00001000 00001400 00000200 00000000
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ


Process Explorer - Sysinternals: www.sysinternals.com [user-PC\user]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 84.20 0 K 24 K 0
procexp64.exe 11.90 9.512 K 20.536 K 2108 Sysinternals Process Explorer Sysinternals - www.sysinter...
Interrupts 2.35 0 K 0 K n/a Hardware Interrupts and DPCs
explorer.exe 0.58 65.732 K 86.952 K 1932 Esplora risorse Microsoft Corporation
VBoxService.exe 0.41 1.944 K 7.528 K 652 VirtualBox Guest Additions S... Oracle Corporation
lsass.exe 0.17 3.588 K 9.920 K 476 Local Security Authority Proc... Microsoft Corporation
System 0.16 136 K 1.192 K 4
VBoxTray.exe 0.11 2.048 K 7.004 K 2020 VirtualBox Guest Additions Tr... Oracle Corporation
csrss.exe 0.04 1.792 K 7.496 K 380
MultiMon.exe 0.02 320.492 K 321.840 K 912
wmpnetwk.exe 0.01 9.944 K 4.948 K 2464 Servizio di condivisione in ret... Microsoft Corporation
lsm.exe 0.01 2.140 K 3.952 K 484
svchost.exe 0.01 16.560 K 18.176 K 792 Processo host per servizi di ... Microsoft Corporation
svchost.exe 0.01 10.888 K 13.788 K 364 Processo host per servizi di ... Microsoft Corporation
SearchIndexer.exe 0.01 18.320 K 14.812 K 1072 Microsoft Windows Search I... Microsoft Corporation
iexplore.exe < 0.01 14.348 K 28.268 K 1048 Internet Explorer Microsoft Corporation
svchost.exe < 0.01 17.504 K 31.424 K 884 Processo host per servizi di ... Microsoft Corporation
csrss.exe < 0.01 1.684 K 3.656 K 320
WmiPrvSE.exe 2.272 K 6.096 K 2608
winlogon.exe 2.396 K 6.428 K 408
wininit.exe 1.292 K 4.184 K 368
taskhost.exe 7.788 K 8.888 K 1220 Processo host per attività di ... Microsoft Corporation
taskeng.exe 1.736 K 5.360 K 2744 Modulo di gestione dell'Utilità... Microsoft Corporation

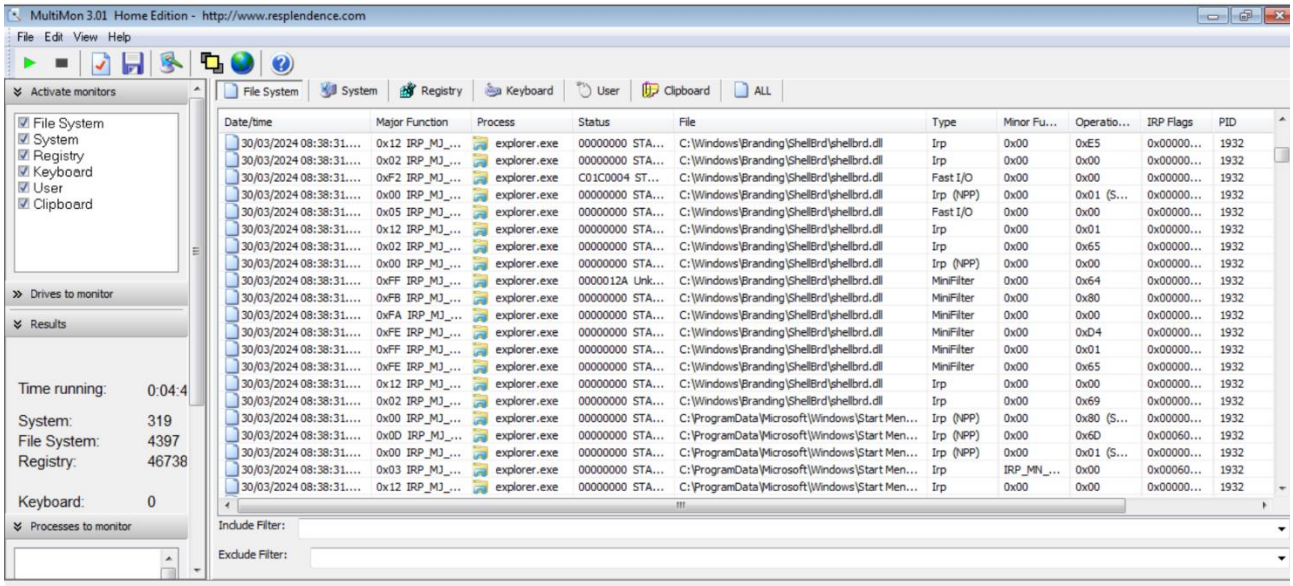

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\wininet.dll SUCCESS Offset: 976.896, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\wininet.dll SUCCESS Offset: 960.512, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\wininet.dll SUCCESS Offset: 919.552, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\wininet.dll SUCCESS Offset: 935.936, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\wininet.dll SUCCESS Offset: 911.360, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\wininet.dll SUCCESS Offset: 993.280, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\profapi.dll SUCCESS Offset: 40.448, Len...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\rasapi32.dll SUCCESS Offset: 373.248, Le...
08:37:... iexplore.exe 1048 IRP_MJ_READ C:\Windows\System32\rasapi32.dll SUCCESS Offset: 360.448, Le...
08:37:... iexplore.exe 1048 IRP_MJ_CREA... C:\Users\user\AppData\Roaming\Micr... SUCCESS Desired Access: R...
08:37:... iexplore.exe 1048 IRP_MJ_CLEA... C:\Users\user\AppData\Roaming\Micr... SUCCESS
08:37:... iexplore.exe 1048 IRP_MJ_CLOSE C:\Users\user\AppData\Roaming\Micr... SUCCESS
08:37:... iexplore.exe 1048 IRP_MJ_CREA... C:\Users\user\AppData\Roaming\Micr... SUCCESS Desired Access: R...
08:37:... iexplore.exe 1048 IRP_MJ_DIRE... C:\Users\user\AppData\Roaming\Micr... SUCCESS Type: QueryDirect...
08:37:... iexplore.exe 1048 IRP_MJ_CLEA... C:\Users\user\AppData\Roaming\Micr... SUCCESS
08:37:... iexplore.exe 1048 IRP_MJ_CLOSE C:\Users\user\AppData\Roaming\Micr... SUCCESS
08:37:... iexplore.exe 1048 IRP_MJ_CREA... C:\Users\user\AppData\Roaming\Micr... SUCCESS Desired Access: R...

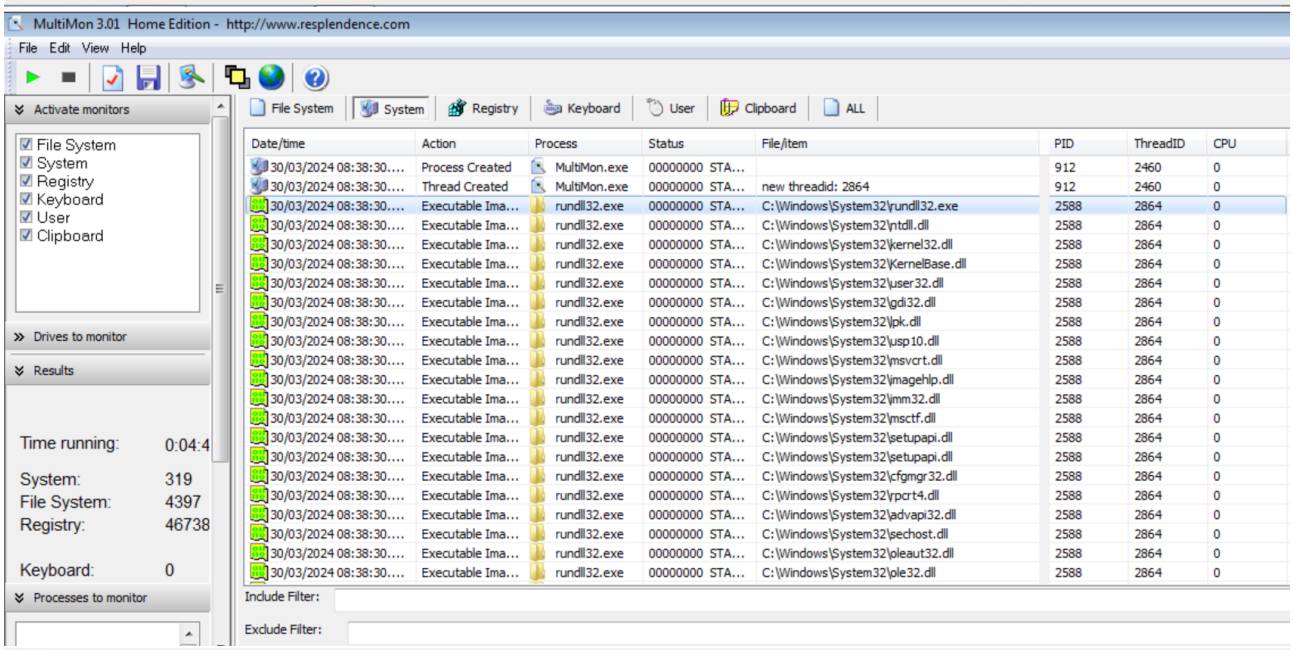

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\mshtml.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\msls31.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Thread Create SUCCESS Thread ID: 2952
08:37:... iexplore.exe 1048 Thread Exit SUCCESS Thread ID: 2952, ...
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\ieapfltr.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\secur32.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Thread Create SUCCESS Thread ID: 2956
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\iepeers.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\winspool.drv SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\msimtf.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\jscript.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Thread Create SUCCESS Thread ID: 2976
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\imgutil.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 1048 Thread Create SUCCESS Thread ID: 1160
08:37:... iexplore.exe 1048 Load Image C:\Windows\System32\pngfilt.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 2428 Load Image C:\Windows\System32\msxml3.dll SUCCESS Image Base: 0x7fef...
08:37:... iexplore.exe 2428 Thread Create SUCCESS Thread ID: 2964
08:37:... iexplore.exe 2428 Thread Exit SUCCESS Thread ID: 2756, ...

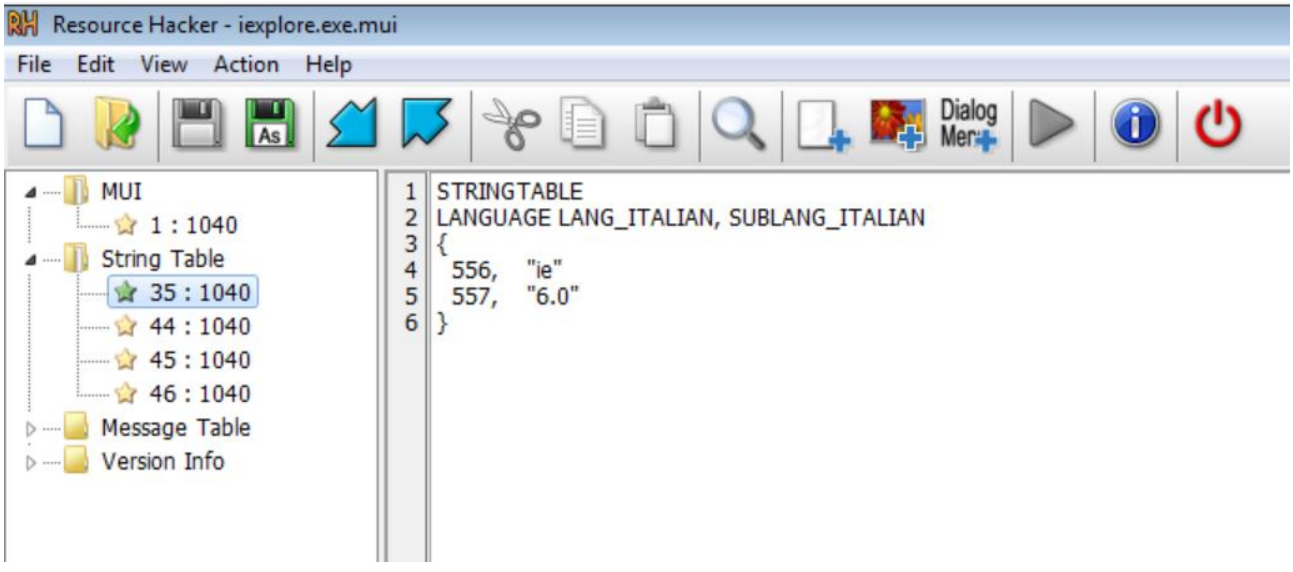


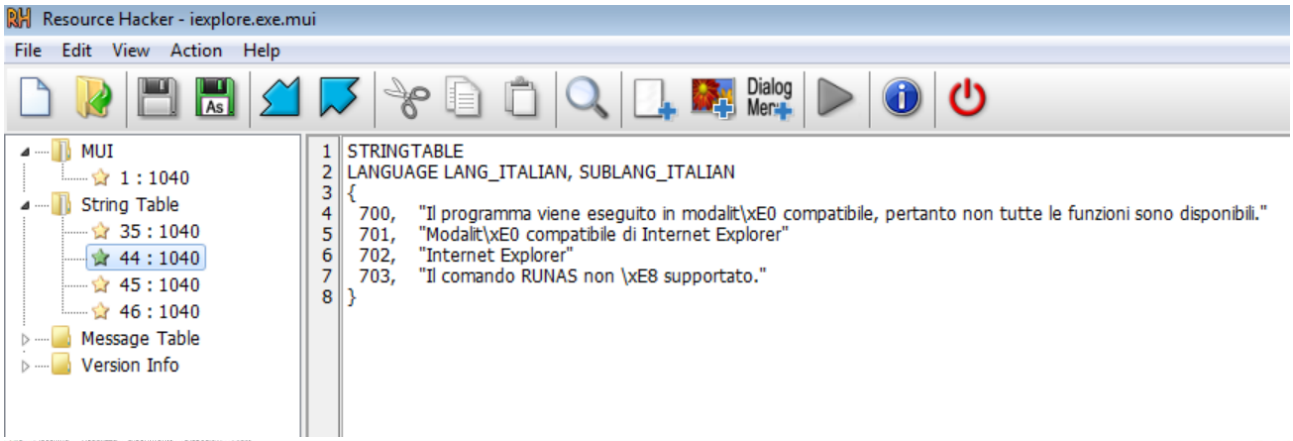
Time ...	Process Name	PID	Operation	Path	Result	Detail
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 144
08:37:...	iexplore.exe	1048	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\Software\Policies\Microsoft\Inte...	NAME NOT FOUND	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKCU\Software\Policies\Microsoft\Inte...	NAME NOT FOUND	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\Software\Microsoft\Internet Expl...	SUCCESS	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKCU\Software\Microsoft\Internet Expl...	NAME NOT FOUND	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Inter...	NAME NOT FOUND	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\Software\Microsoft\Internet Expl...	SUCCESS	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Inter...	NAME NOT FOUND	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\Software\Microsoft\Internet Expl...	SUCCESS	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Inter...	NAME NOT FOUND	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\Software\Microsoft\Internet Expl...	SUCCESS	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	Query: HandleTag...
08:37:...	iexplore.exe	1048	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Inter...	SUCCESS	Desired Access: Q...
08:37:...	iexplore.exe	1048	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Inter...	NAME NOT FOUND	Length: 144
08:37:...	iexplore.exe	1048	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Inter...	NAME NOT FOUND	Length: 144

```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2024/3/30 07:34:57  ,  2024/3/30 07:39:55
Computer: USER-PC , USER-PC
Username: user , user

----------------------------------
Keys deleted: 2
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{7206988A-C46D-4E3A-B05A-704B104EF1F3}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7206988A-C46D-4E3A-B05A-704B104EF1F3}

----------------------------------
Keys added: 47
----------------------------------
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{C6AFEE2A-8FC7-4FAD-93C2-2053166EB793}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{C6AFEE2A-8FC7-4FAD-93C2-2053166EB793}
HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
HKLM\SYSTEM\ControlSet001\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_RSPMMFS\0000\Control
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_RSPMON\0000\Control
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\ControlSet001\services\PROCMON23
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances\Process Monitor 23 Instance
HKLM\SYSTEM\Setup\SetupapiLogStatus
HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_RSPMMFS\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_RSPMON\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances\Process Monitor 23 Instance
```

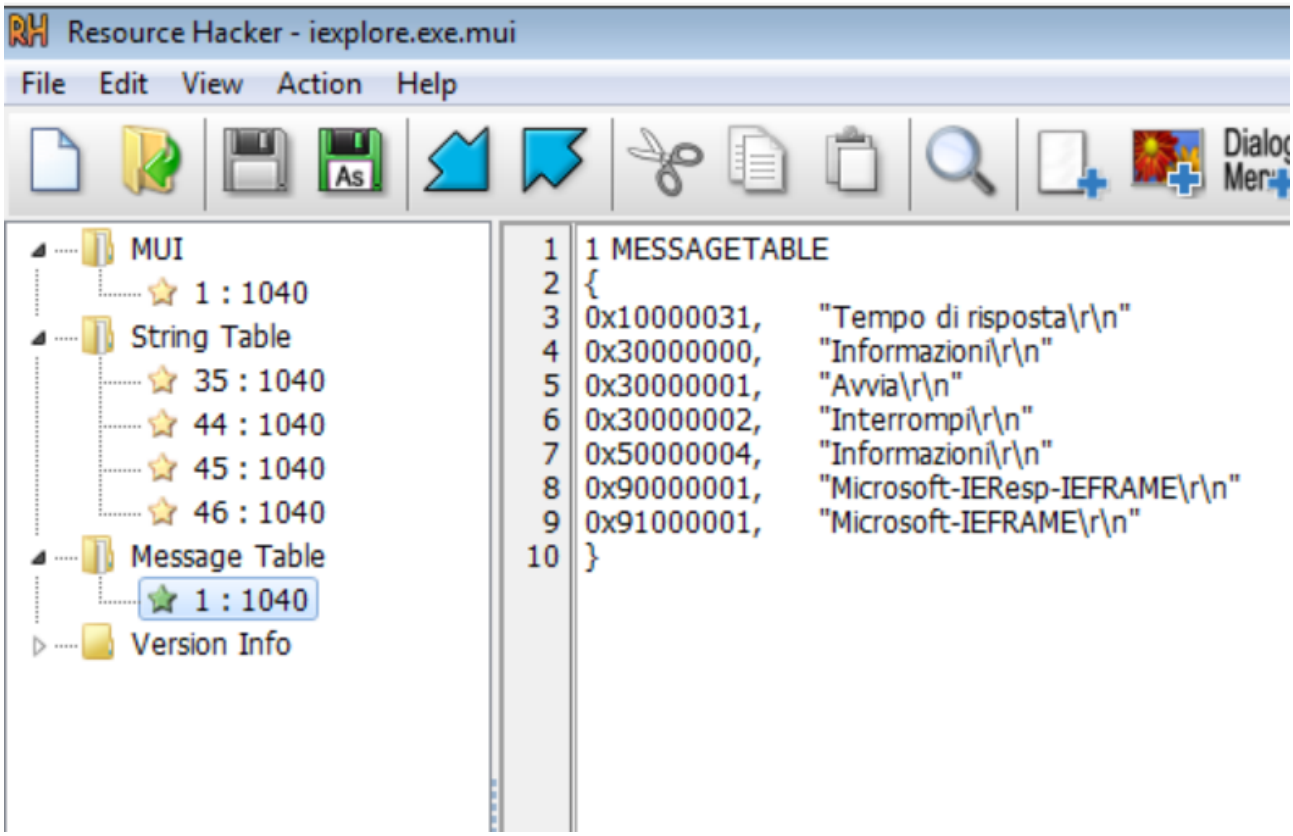

MultiMon 3.01 Home Edition - http://www.resplendence.com
File Edit View Help
Activate monitors
File System
System
Registry
Keyboard
User
Clipboard
Drives to monitor
Results
Time running: 0:04:4
System: 319
File System: 4397
Registry: 46738
Keyboard: 0
Processes to monitor
File System
System
Registry
Keyboard
User
Clipboard
ALL
Date/time
Major Function
Process
Status
File
Type
Minor Fu...
Operatio...
IRP Flags
PID
Include Filter:
Exclude Filter:

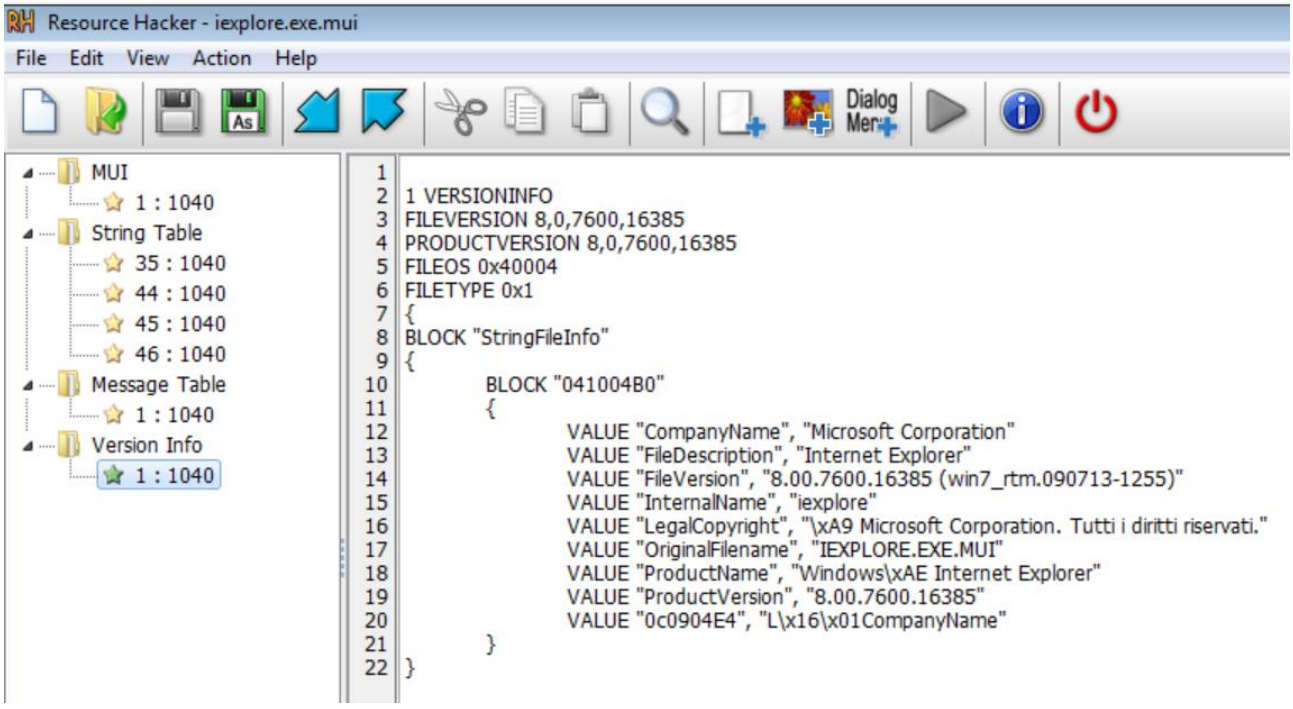

MultiMon 3.01 Home Edition - http://www.resplendence.com
File Edit View Help
Activate monitors
File System
System
Registry
Keyboard
User
Clipboard
Drives to monitor
Results
Time running: 0:04:4
System: 319
File System: 4397
Registry: 46738
Keyboard: 0
Processes to monitor
File System
System
Registry
Keyboard
User
Clipboard
ALL
Date/time
Action
Process
Status
File/item
PID
ThreadID
CPU
Include Filter:
Exclude Filter:


Resource Hacker - iexplore.exe.mui
File Edit View Action Help
MUI
1 : 1040
String Table
35 : 1040
44 : 1040
45 : 1040
46 : 1040
Message Table
Version Info
1 STRINGTABLE
2 LANGUAGE LANG_ITALIAN, SUBLANG_ITALIAN
3 {
4 556, "ie"
5 557, "6.0"
6 }


Resource Hacker - iexplore.exe.mui
File Edit View Action Help
MUI
1 : 1040
String Table
35 : 1040
44 : 1040
45 : 1040
46 : 1040
Message Table
Version Info
1 STRINGTABLE
2 LANGUAGE LANG_ITALIAN, SUBLANG_ITALIAN
3 {
4 700, "Il programma viene eseguito in modalit\xE0 compatibile, pertanto non tutte le funzioni sono disponibili."
5 701, "Modalit\xE0 compatibile di Internet Explorer"
6 702, "Internet Explorer"
7 703, "Il comando RUNAS non \xE8 supportato."
8 }


Resource Hacker - iexplore.exe.mui
File Edit View Action Help
String Table : 45 : 1040
MUI
1 : 1040
String Table
35 : 1040
44 : 1040
45 : 1040
46 : 1040
Message Table
Version Info
1 STRINGTABLE
2 LANGUAGE LANG_ITALIAN, SUBLANG_ITALIAN
3 {
4 705, "Per avviare Internet Explorer in questo computer \xE8 necessario essere un amministratore.\n\nPer avviare Internet Explorer, fare clic con il pulsante destro del mouse sull'icona di Ir
5 706, "Con Windows Internet Explorer 8 \xE8 possibile esplorare il Web in modo ancora pi\xF9 semplice e sicuro, eseguire ricerche rapide direttamente dalla barra degli strumenti, eseguire s
6 707, "Per il corretto funzionamento di Internet Explorer 8 \xE8 necessario un aggiornamento per la sicurezza Windows.\n\nFare clic su OK per scaricare l'aggiornamento per la sicurezza Wir
7 }


Resource Hacker - iexplore.exe.mui
File Edit View Action Help
MUI
1 : 1040
String Table
35 : 1040
44 : 1040
45 : 1040
46 : 1040
Message Table
1 : 1040
Version Info
1 MESSAGETABLE
{
0x10000031, "Tempo di risposta\r\n"
0x30000000, "Informazioni\r\n"
0x30000001, "Avvia\r\n"
0x30000002, "Interrompi\r\n"
0x50000004, "Informazioni\r\n"
0x90000001, "Microsoft-IEResp-IEFRAME\r\n"
0x91000001, "Microsoft-IEFRAME\r\n"
}


Resource Hacker - iexplore.exe.mui
File Edit View Action Help
MUI
1 : 1040
String Table
35 : 1040
44 : 1040
45 : 1040
46 : 1040
Message Table
1 : 1040
Version Info
1 : 1040
1 VERSIONINFO
FILEVERSION 8,0,7600,16385
PRODUCTVERSION 8,0,7600,16385
FILEOS 0x40004
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
BLOCK "041004B0"
{
VALUE "CompanyName", "Microsoft Corporation"
VALUE "FileDescription", "Internet Explorer"
VALUE "FileVersion", "8.00.7600.16385 (win7_rtm.090713-1255)"
VALUE "InternalName", "iexplore"
VALUE "LegalCopyright", "\xA9 Microsoft Corporation. Tutti i diritti riservati."
VALUE "OriginalFilename", "IEXPLORE.EXE.MUI"
VALUE "ProductName", "Windows\xAE Internet Explorer"
VALUE "ProductVersion", "8.00.7600.16385"
VALUE "0c0904E4", "L\x16\x01CompanyName"
}
}