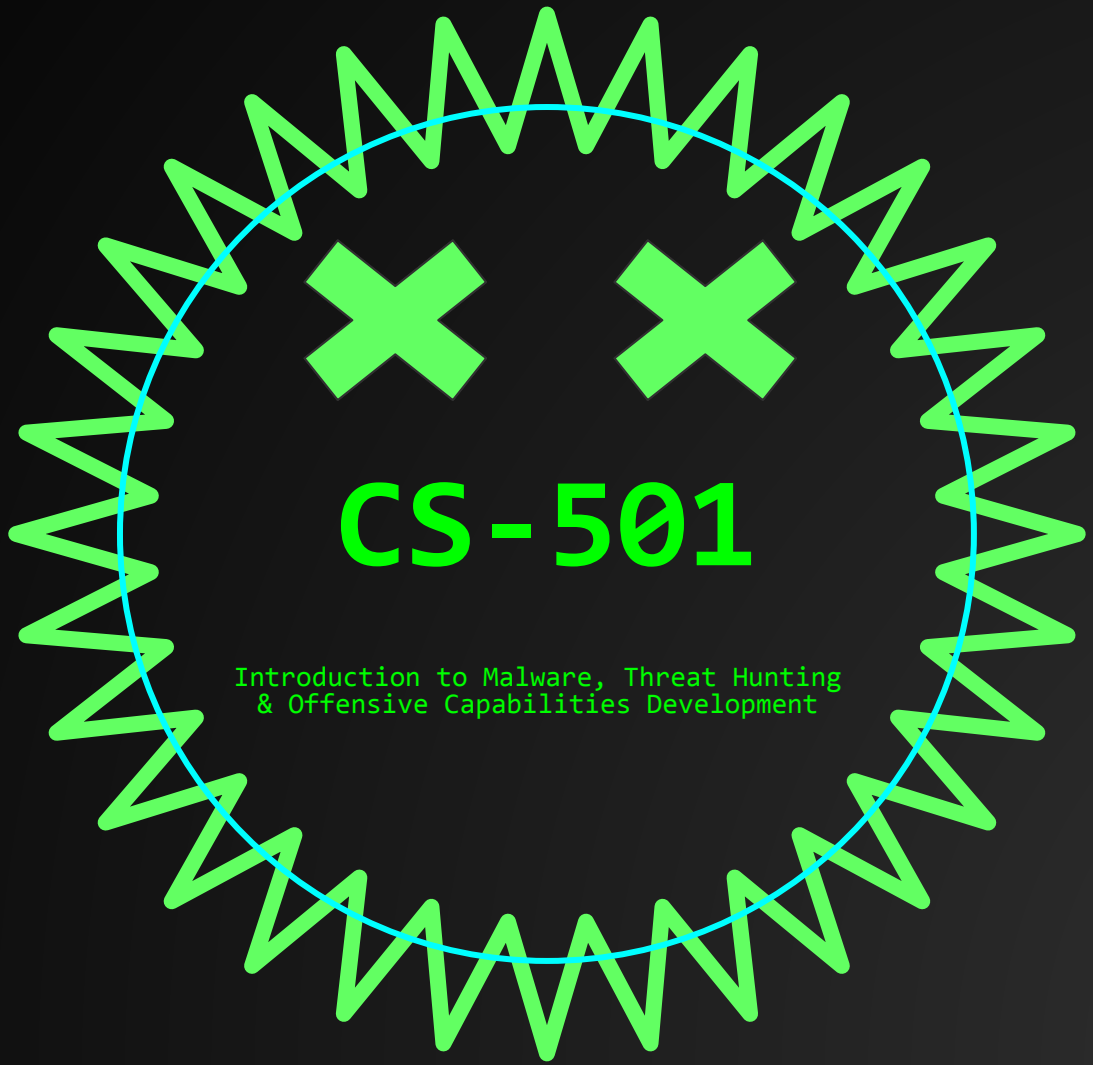


CS-501

Introduction to Malware, Threat Hunting
& Offensive Capabilities Development

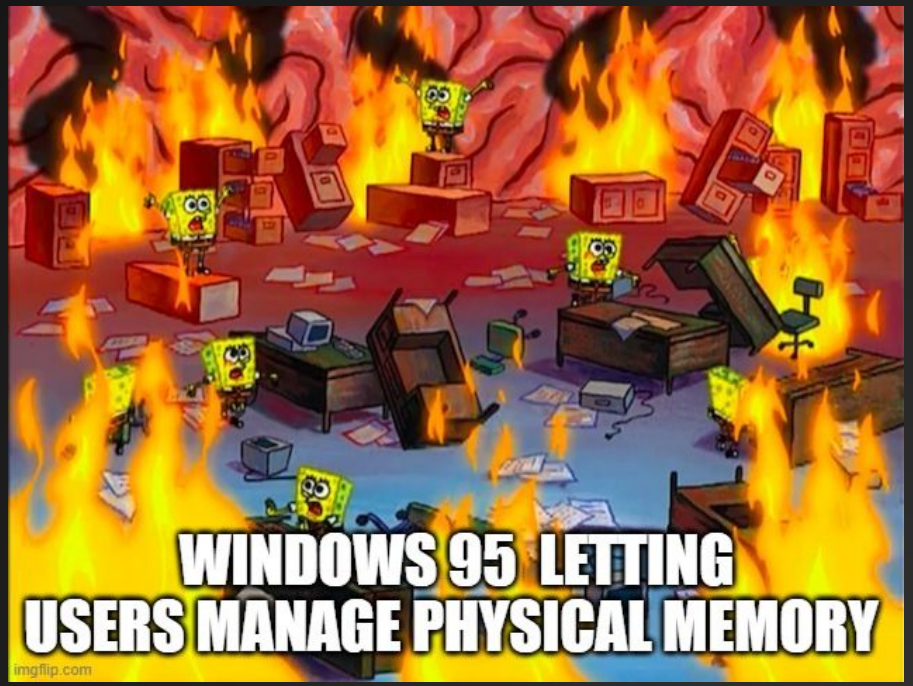
Lecture 7
Windows Internals: Files & I/O

Review: Kernel Objects

- Objects are created and managed by the *Kernel Object Manager*
- The Object Manager lives in kernel space and is beyond the scope of this lecture. That said…
- The object manager maintains a count of the number of references to an object.
- When an object is created, the object manager sets the object's reference count to one.
- Once that counter falls to zero, the object is freed.
- When a processes ends (or crashes), all of its handles are destroyed
- Creating an object usually involves a win32 api call Create[ObjectName]

Why do we interact with Objects via Handles?

- If you mess something up in a processes, it might hoard resources/crash. The resources used by the process are cleaned up when it terminates.
- If you mess something up in kernel space, resources might be locked until a reboot, or you could get an instant BSOD.
- Access control is also a plus



More on Kernel Objects

The Object Manager is responsible for (among other things)

- Creation and destruction of objects
- Controlling access
- Maintaining a list of which processes is using what object
- Managing object lifetimes: i.e. when is it safe to auto-destroy an object?

Kernel Object Examples

- Files
- Threads
- Processes
- Devices
- Mutexes
- Symbolic links
- Access Tokens

Viewing Handle Usage

Sysinternals Handle64

```
PS C:\tools\sysinternals> .\handle.exe /help

Nthandle v4.22 - Handle viewer
Copyright (C) 1997-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: handle [[-a [-l]] [-u] | [-c <handle> [-y]] | [-s]] [-p <process>|<pid>] [name] [-nobanner]
  -a         Dump all handle information.
  -l         Just show pagefile-backed section handles.
  -c         Closes the specified handle (interpreted as a hexadecimal number).
             You must specify the process by its PID.
             WARNING: Closing handles can cause application or system instability.
  -y         Don't prompt for close handle confirmation.
  -s         Print count of each type of handle open.
  -u         Show the owning user name when searching for handles.
  -p         Dump handles belonging to process (partial name accepted).
  name       Search for handles to objects with <name> (fragment accepted).
  -nobanner  Do not display the startup banner and copyright message.

No arguments will dump all file references.
PS C:\tools\sysinternals> .\handle.exe -p brave.exe

Nthandle v4.22 - Handle viewer
Copyright (C) 1997-2019 Mark Russinovich
Sysinternals - www.sysinternals.com
```

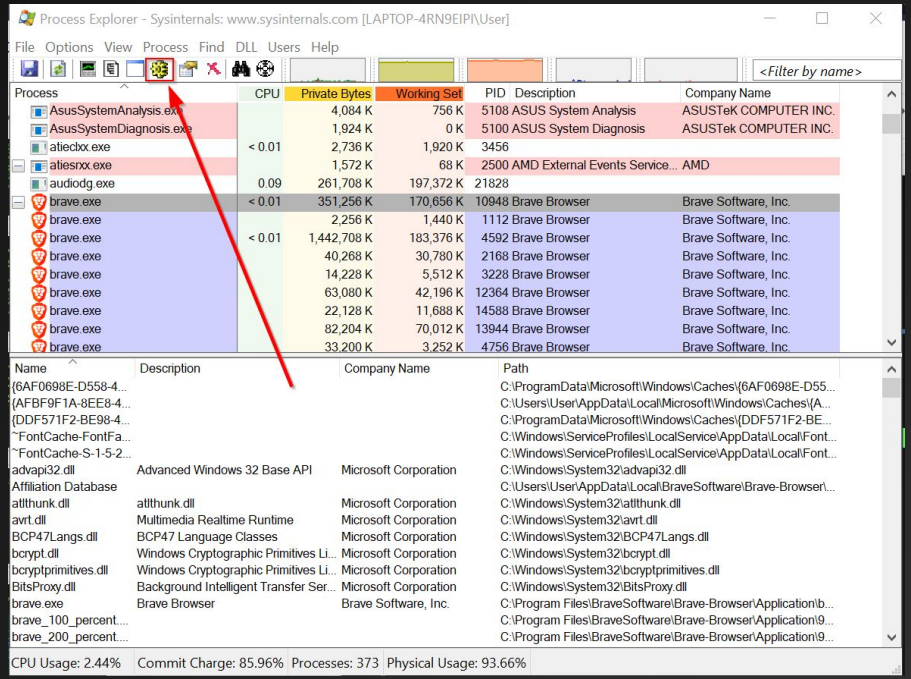
Example:

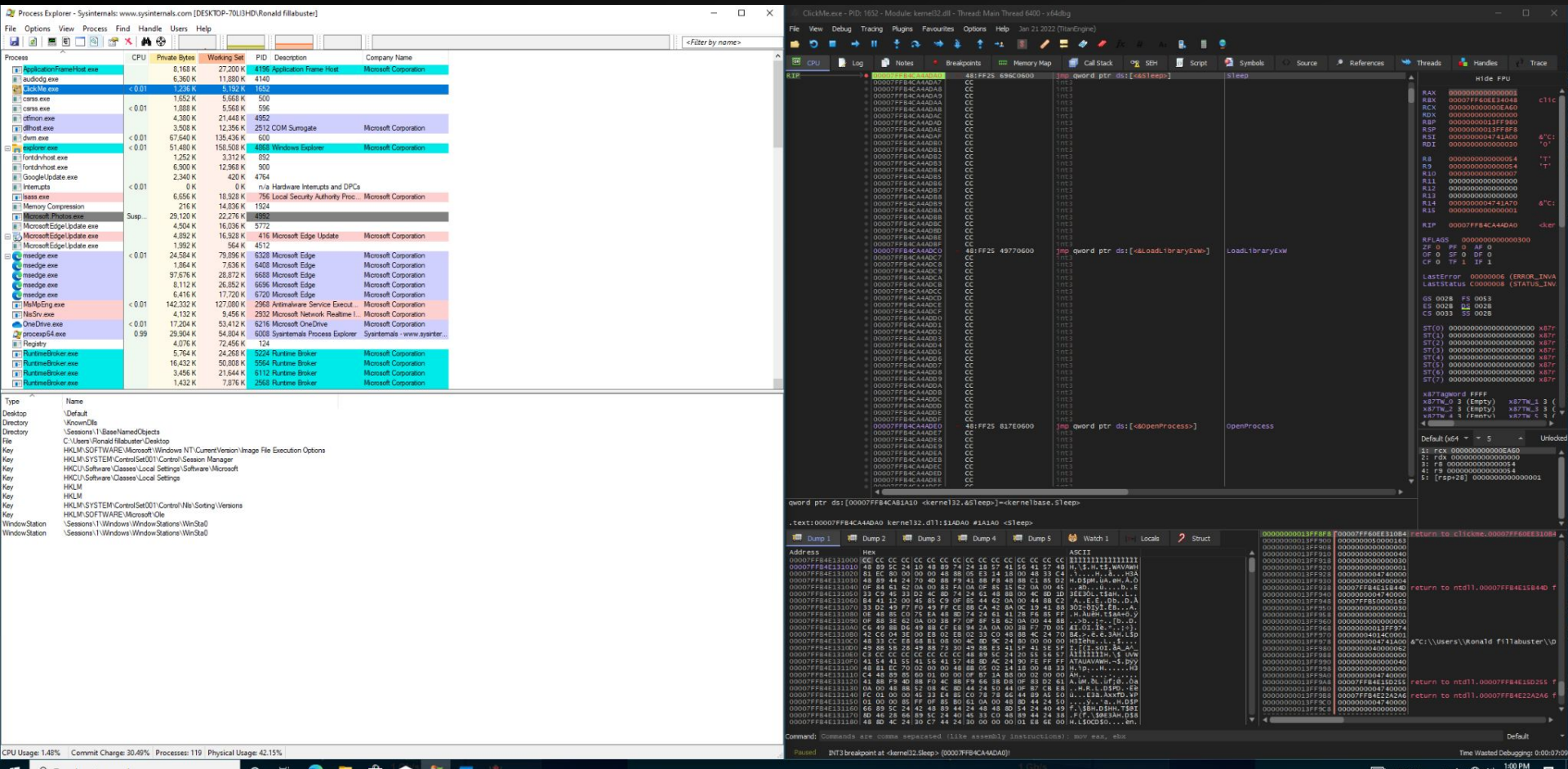
```
.\handle64.exe  -p brave.exe
```

```
PS C:\tools\sysinternals> .\handle64.exe  -p brave.exe

Nthandle v4.22 - Handle viewer
Copyright (C) 1997-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

------------------------------------------------------------------------------
brave.exe pid: 10948 LAPTOP-4RN9EIPI\User
   70: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101
  200: Section       \Sessions\1\BaseNamedObjects\windows_shell_global_counters
  2F8: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\icudtl.dat
  3A8: File          C:\Users\User\AppData\Local\BraveSoftware\Brave-Browser\User Data\BrowserMetrics\BrowserMetrics-620A6E26-2AC4.pma
  3B0: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\chrome_100_percent.pak
  3B8: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\chrome_200_percent.pak
  3C0: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\Locales\en-US.pak
  3C8: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\resources.pak
  3D0: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\brave_resources.pak
  3D8: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\brave_100_percent.pak
  3E0: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101\brave_200_percent.pak
  420: File          C:\Users\User\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\Local Extension Settings\mnojpmjdmbbfmejpflffi
fhffcmidifd\LOCK
  4A8: File          C:\Program Files\BraveSoftware\Brave-Browser\Application\98.1.35.101
  524: File          C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.1110_none_60b5254171f9507e
  5B0: Section       \Windows\Theme1197514762
  5B4: Section       \Sessions\1\Windows\Theme4022028298
  5C0: Section       \BaseNamedObjects\__ComCatalogCache__
  5CC: Section       \BaseNamedObjects\__ComCatalogCache__
  5D0: File          C:\Windows\Registration\R000000000007.clb
  654: Section       \Sessions\1\BaseNamedObjects\2ac4HWNDInterface:80072
```

Process Explorer

- Task manager on steroids
- Provides information about processes, parent/child relationships, Handles, DLLs, in memory strings… and more!
- To View handle we click




Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-70LI3HD\Ronald fillabuster]
ClickMe.exe - PID: 1652 - Module: kernel32.dll - Thread: Main Thread 6400 - x64dbg
Windows Task Manager
Type here to search
17°F Clear
1:00 PM
2/14/2022

File Objects

- File Objects are a type of Kernel Objects
- “File objects function as the logical interface between kernel and user-mode processes and the file data that resides on the physical disk.”
- File Object != Disk file, but all disk files are File Objects
- Files on the filesystem (most of the time) are actually symbolic links to some file saved on a physical disk

The Windows I/O System

- Any (useful) operating system needs to be able to interact with external entities called “devices”
- By interact, I mean receive input and send output to external devices.
- For example, our PCs wouldn’t be very useful to us without the ability to send keystrokes via a keyboard, and have the computer display output to the screen
- A *driver* provides a *software interface* for the exchange of data between the device and OS
- The Windows I/O manager is a kernel feature that “manages the communication between applications and the interfaces provided by device drivers”
- In other words, the IO system abstracts away complicated, and dangerous parts of performing I/O on physical and logical devices

Windows I/IO system: Userland perspective

- Userland processes call into the I/O system using the Windows (or Native) API
- Any File I/O operation is initiated by a kernel mode entity within the I/O system called the *I/O Manager*
- In order to initiate this processes, the Native API invokes a *syscall*
- Recall that a syscall is the lowest level, userland function available to us: this allows userland processes to call into Kernel space via an API

The Windows File system

- From the perspective of an application/user, files are organized in a Tree structure
- There are many different types of files, but the basic ones are directories, and Regular files
- Directories can have child nodes
- Regular files cannot have child nodes

File Paths

- Unix Paths start at the root directory “/”
- A path is either a *relative* or *absolute* path to a file
- Example: “../folder_a/file_a.txt” is a relative path
- “..” is the previous directory one level out
- “.” is the current directory
- Example: “/home/remnux/Desktop/inetsim.conf” is an absolute path to a file
- On Windows, we use “\” as opposed to “/” for a path separator

Tree Structure

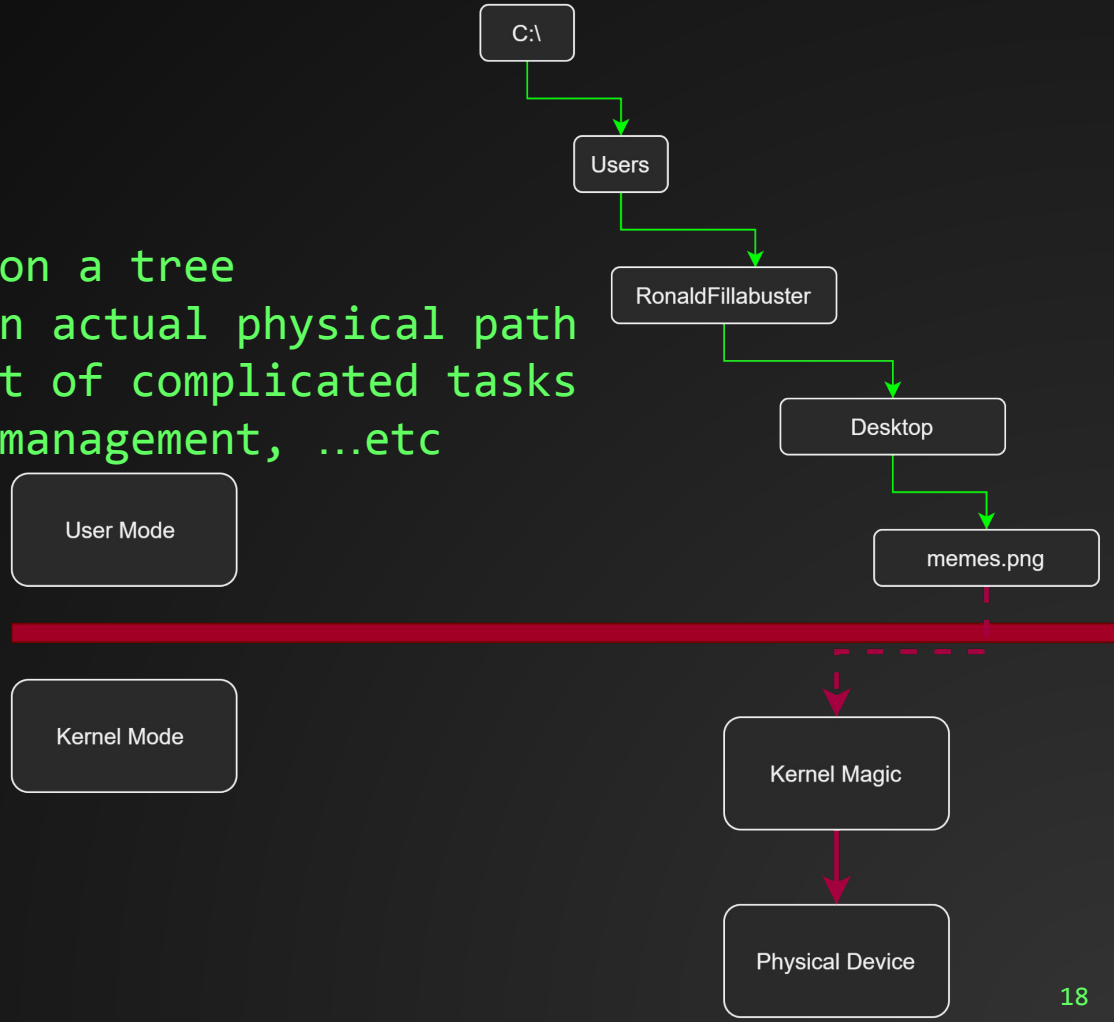
`tree /f .` creates an ASCII art tree representation of the tree structure with root node equal to the current directory

It then “Walks” the tree and displays all files and directories

```
C:\dev\CS-501-malware-course\Assignments>tree /f .
Folder PATH listing for volume OS
Volume serial number is [redacted]
C:\DEV\CS-501-MALWARE-COURSE\ASSIGNMENTS
├───HW0
│       hw0.exe
│
├───HW1
│       activate.c
│       fibonacci.c
│       highground.c
│       Makefile
│       myls.c
│       mystrings.c
│       reverse.c
│
└───HW2
    ├───CrackMes
    │       crackme0.exe
    │       crackme1.exe
    │       crackme2.exe
    │       crackme3.exe
    │       crackme4.exe
    │       crackme5.exe
    │       crackme6.exe
    │       crackme7.exe
    │       crackme8.exe
    │
    └───Suspicious
```

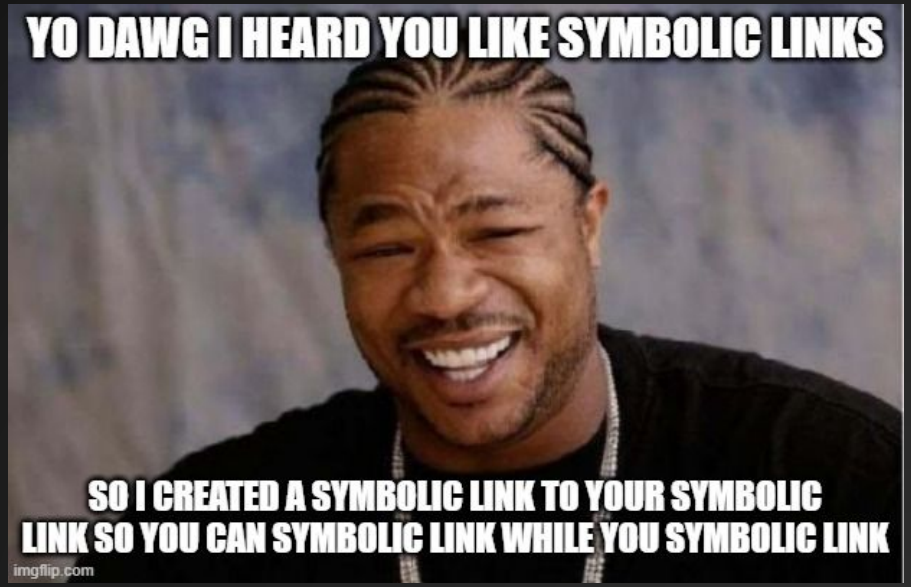
Directory Tree

- Paths are always paths on a tree
- The path is mapped to an actual physical path
- The kernel handles a lot of complicated tasks such as Disk IO, power management, ...etc

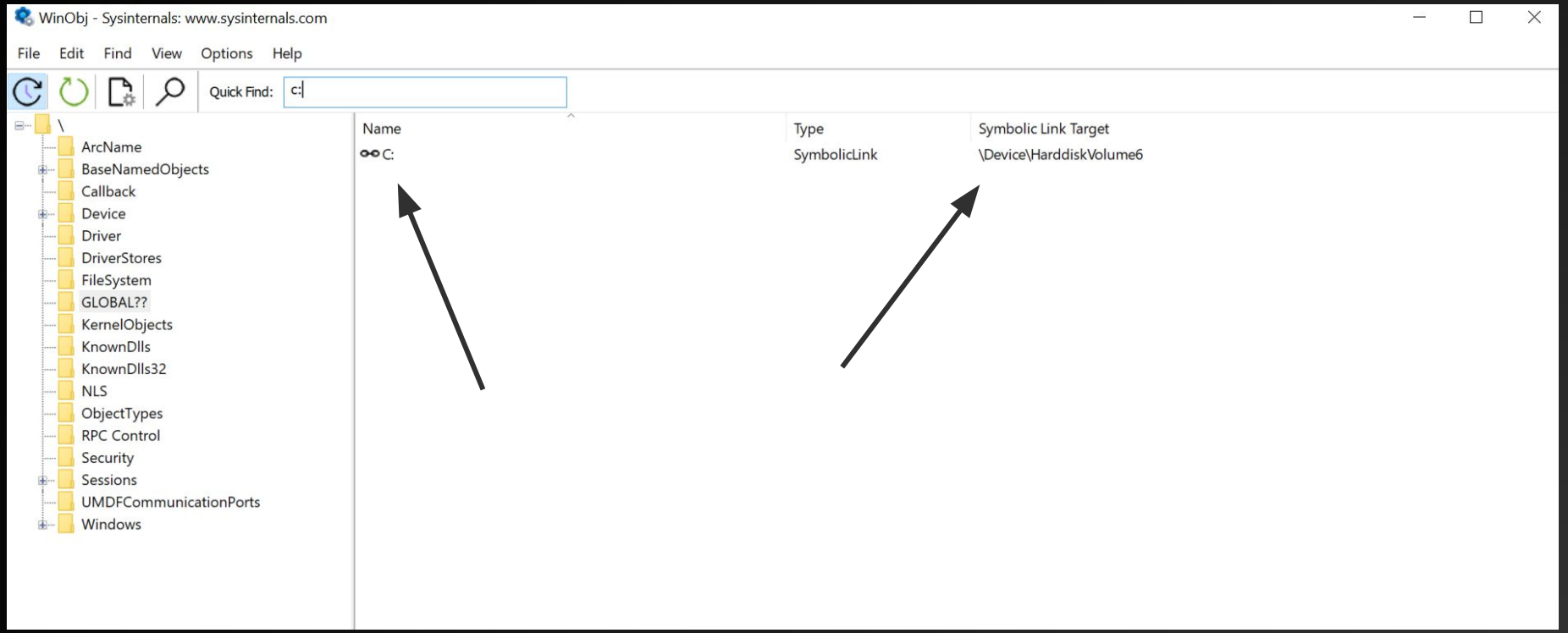


Symbolic Links

- A symbolic link is an alias for a symbolic link target
- On Windows, we usually pass symbolic links as arguments to functions
- Logical drives like C:\ are actually symbolic links to (usually) volumes on a disk
- WinObj64 is a sysinternals tool that allows us to view Kernel objects including Symbolic links



C:\ is a symbolic link



Terminology: Files

In this class, we will use the following Convention for talking about File Objects:

- File: What you normally think of when someone says a file. I.e., something with a symbolic link on disk.
- File Object: A kernel object

If I say File, I mean a file on disk

If I say File Object, I am referring to a Kernel Object

Getting a Handle to a File Object

- CreateFile(A||W): Win32 call to create a handle to a File Object. Supports all versions of Windows.
- CreateFile2: Similar to CreateFileW, but can be called from a special type of Application called a Universal Windows Platform (UWP). Is only supported on Windows 8 and above
- NtCreateFile: Native API call to create a File Object. All of the functions above call into it!

CreateFileA

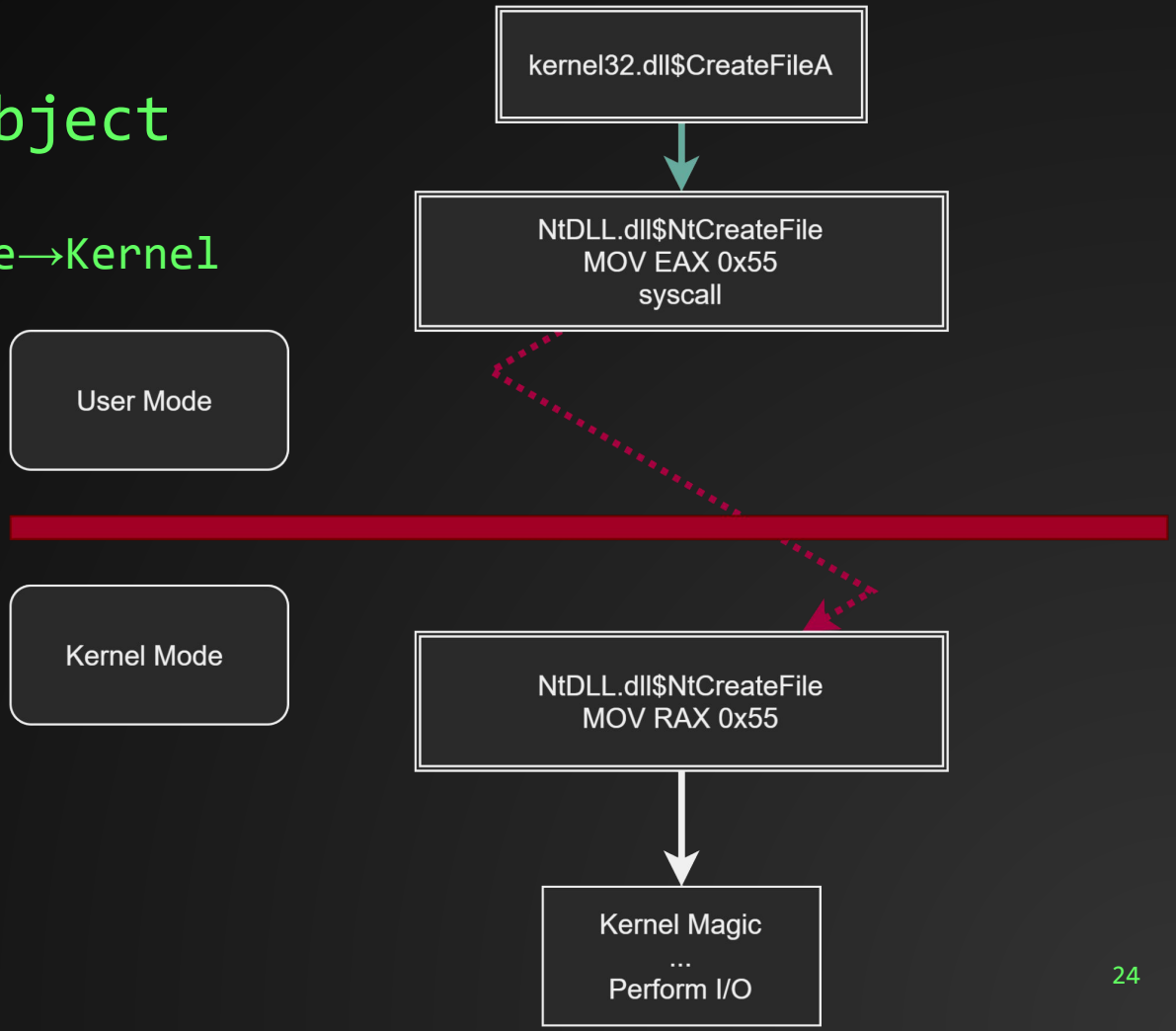
```
HANDLE CreateFileA(
  [in]           LPCSTR                lpFileName,
  [in]           DWORD                 dwDesiredAccess,
  [in]           DWORD                 dwShareMode,
  [in, optional] LPSECURITY_ATTRIBUTES lpSecurityAttributes,
  [in]           DWORD                 dwCreationDisposition,
  [in]           DWORD                 dwFlagsAndAttributes,
  [in, optional] HANDLE                hTemplateFile
);
```

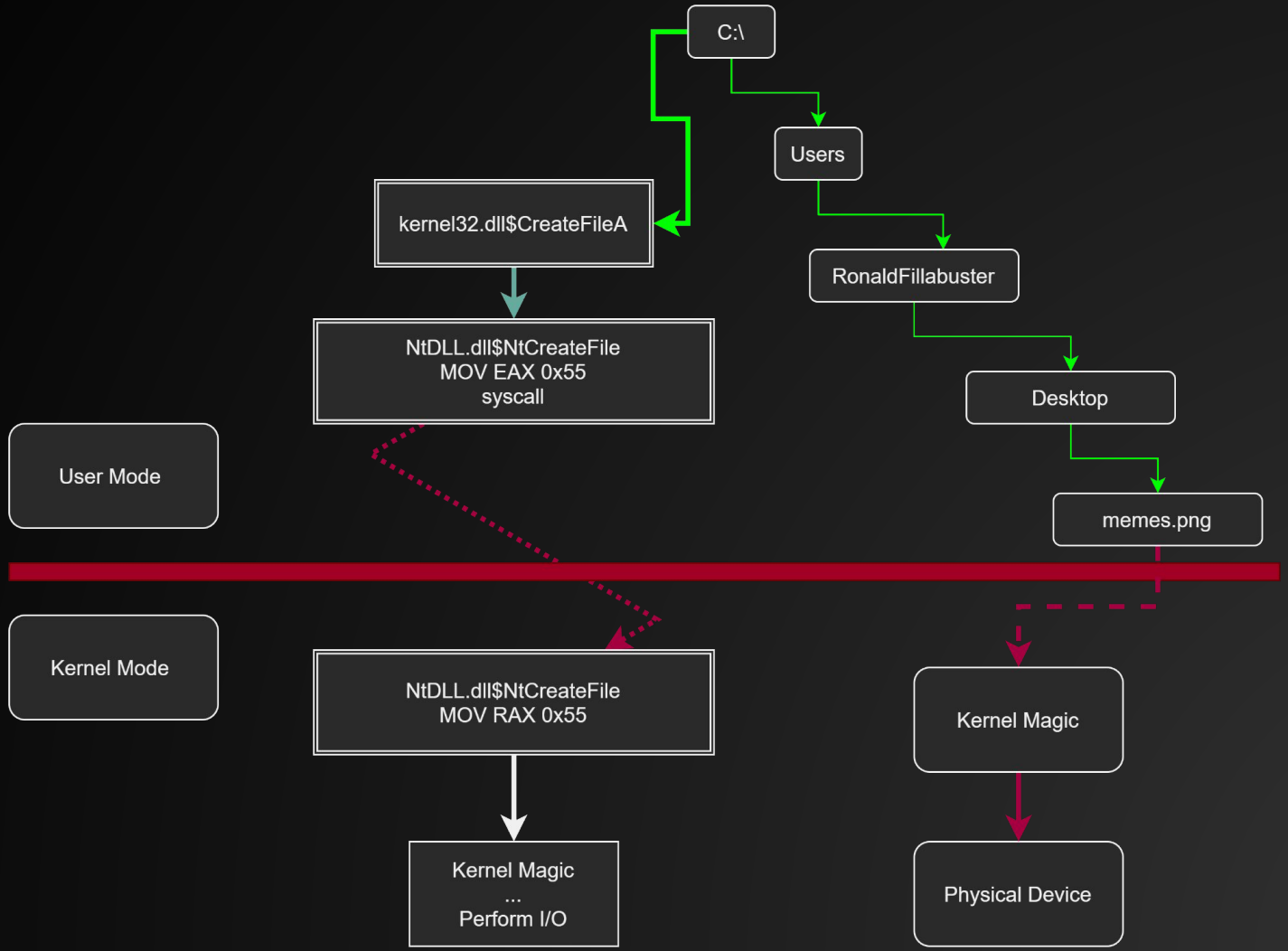
- Demo: reading the Docs
- https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilea

Creating a File Object

CreateFileA→NtCreateFile→Kernel Magic

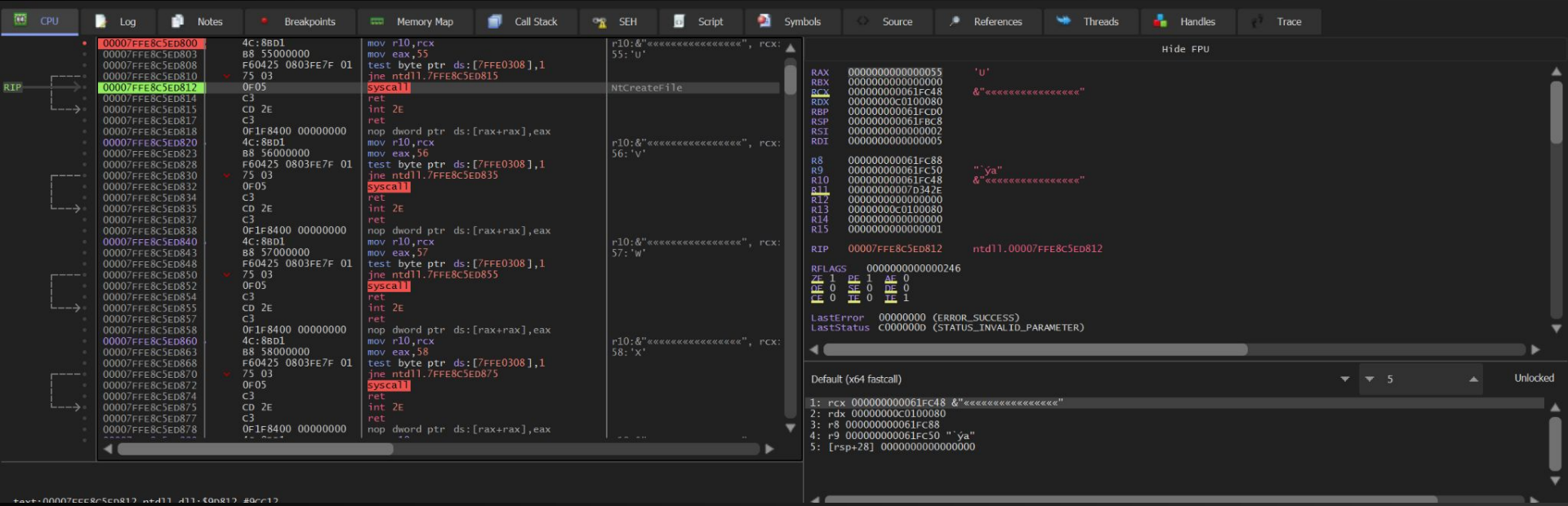
I/O System abstraction




C:\
Users
RonaldFillabuster
Desktop
memes.png
kernel32.dll$CreateFileA
NtDLL.dll$NtCreateFile
MOV EAX 0x55
syscall
User Mode
Kernel Mode
NtDLL.dll$NtCreateFile
MOV RAX 0x55
Kernel Magic
...
Perform I/O
Kernel Magic
Physical Device

NtCreateFile

00007FFE8C5ED812 | 0F05 | syscall | NtCreateFile

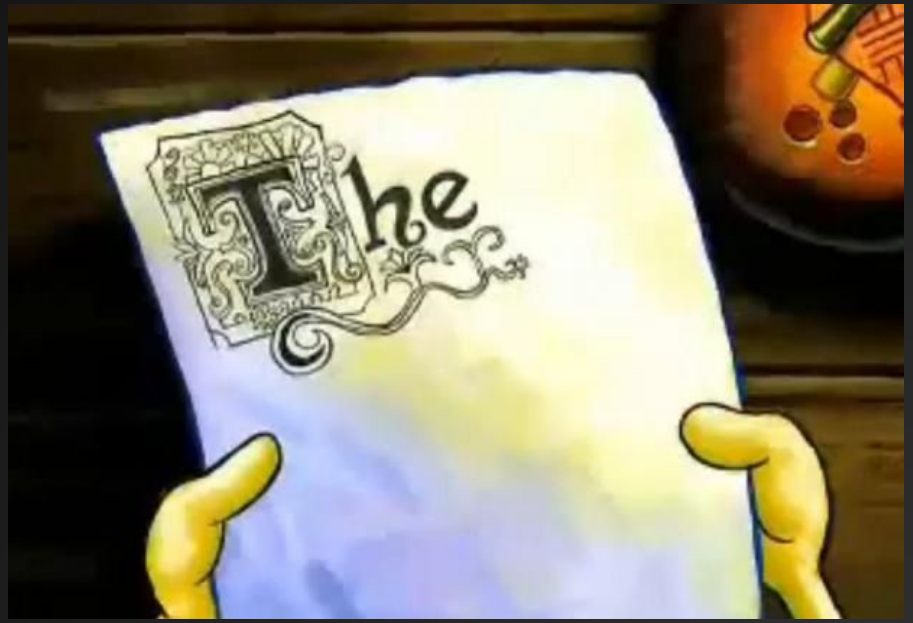


Mapping Symbolic Links to Target paths

```
DWORD QueryDosDeviceA(
  [in, optional] LPCSTR lpDeviceName,
  [out]          LPSTR  lpTargetPath,
  [in]           DWORD  ucchMax
)
```

Querying File Information

- Calculating the File Size
- Reading/modifying file “times”
- Reading/modifying File Attributes
- How? You will figure it out on your homework :D

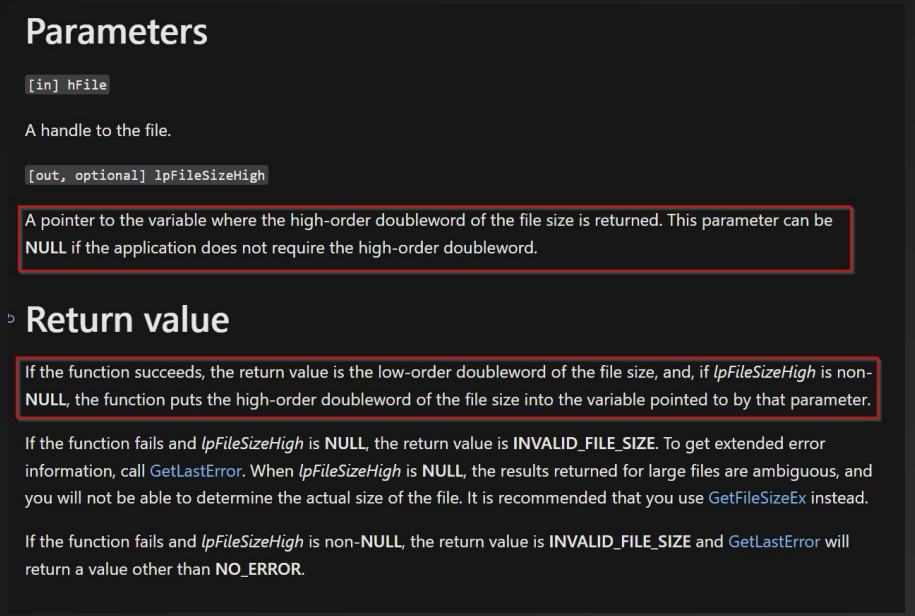


File Attributes

- Metadata associated with file objects committed to disk
- When creating Files, you can control these attributes with File Attribute masks
- Examples:
  - `FILE_ATTRIBUTE_NORMAL` The mask you use for normal files
  - `FILE_ATTRIBUTE_DIRECTORY` The file is a directory
  - `FILE_ATTRIBUTE_HIDDEN` The file is hidden
  - `FILE_ATTRIBUTE_NOT_CONTENT_INDEXED` The file won't be indexed
  - `FILE_ATTRIBUTE_READONLY` The file is read only.
  - `FILE_ATTRIBUTE_TEMPORARY` File attempts to stay in memory.
- Full:https://docs.microsoft.com/en-us/windows/win32/fileio/file-attribute-constants

Common Footguns

- DWORD is an unsigned 32 bit integer
- When Windows NT was first rolled out, the thought of having lots of files larger than 2^32 bytes was a bit of an insane/edge case prospect
- 2^32 bytes is about 4.3 Gigabytes
- On the other hand, 2^64 bytes is about 1.8 * 10^10 gigabytes
  - Or 18,446,744.1 terabytes. That is pretty large. For now, 64bit unsigned integers should be sufficient to house file sizes
- GetFileSize returns a 32bit unsigned integer
- If it is larger than 4gbs, then you need to use lpFileSizeHigh
- If you set lpFileSizeHigh to null, and fs>4gb…you will have a bad time
- Please use GetFileSizeEx



Parameters

`[in] hFile`

A handle to the file.

`[out, optional] lpFileSizeHigh`

A pointer to the variable where the high-order doubleword of the file size is returned. This parameter can be **NULL** if the application does not require the high-order doubleword.

Return value

If the function succeeds, the return value is the low-order doubleword of the file size, and, if *lpFileSizeHigh* is non-**NULL**, the function puts the high-order doubleword of the file size into the variable pointed to by that parameter.

If the function fails and *lpFileSizeHigh* is **NULL**, the return value is **INVALID_FILE_SIZE**. To get extended error information, call GetLastError. When *lpFileSizeHigh* is **NULL**, the results returned for large files are ambiguous, and you will not be able to determine the actual size of the file. It is recommended that you use GetFileSizeEx instead.

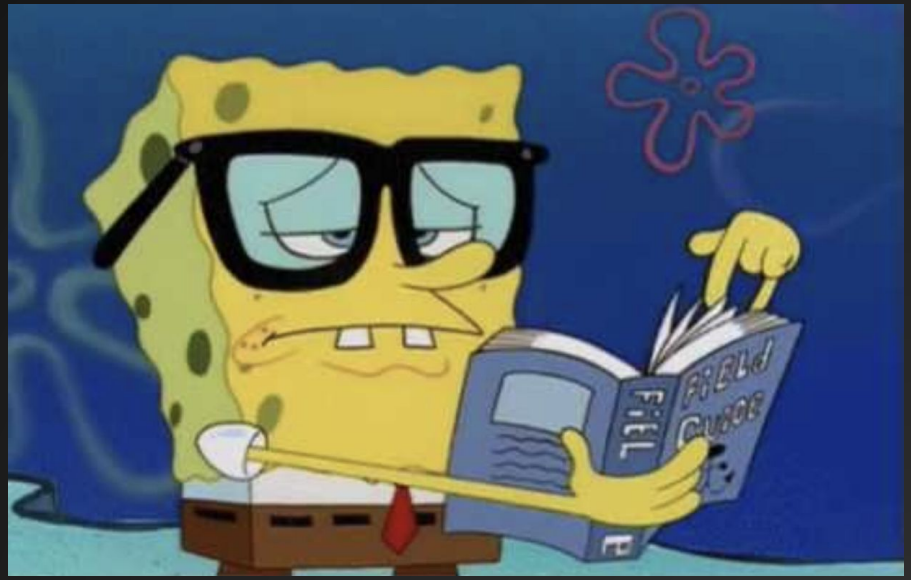
If the function fails and *lpFileSizeHigh* is non-**NULL**, the return value is **INVALID_FILE_SIZE** and GetLastError will return a value other than **NO_ERROR**.

Synchronous File IO

- Windows performs I/O asynchronously under the hood
- That said, async I/O is considerably more complicated than Synchronous I/O
- Here synchronous means the thread performing I/O is blocked (in a waiting state) until the I/O is completed
- Async allows the the thread to go do other work while it waits for the I/O to finish
- For now, we will only look at Synchronous I/O

File I/O: Reading

- Like everything involving I/O, we first call CreateFile
- You should then determine the size of the file
- Allocate a buffer large enough to fit all of the data.
  - If the data is to be interpreted as a string, make sure to have enough space for an added null byte
  - If the file is Unicode encoded, make sure to have enough space for a wide char null terminator!



Remarks on Memory Allocation

- We will dedicate more time to this later on in the class, but you should currently be familiar with C-runtime style memory management. I.e., `malloc` `free`
- C++: new/delete
  - Where as `malloc` only lets you allocate in terms of bytes, new lets you allocate space according to an objects type!
  - I.e., malloc(sizeof(int) * 100) vs new int[100];
- Modern C++: Smart pointers
  - <memory>--> std::make_unique ← smart pointer that is automatically freed once the object goes out of scope!

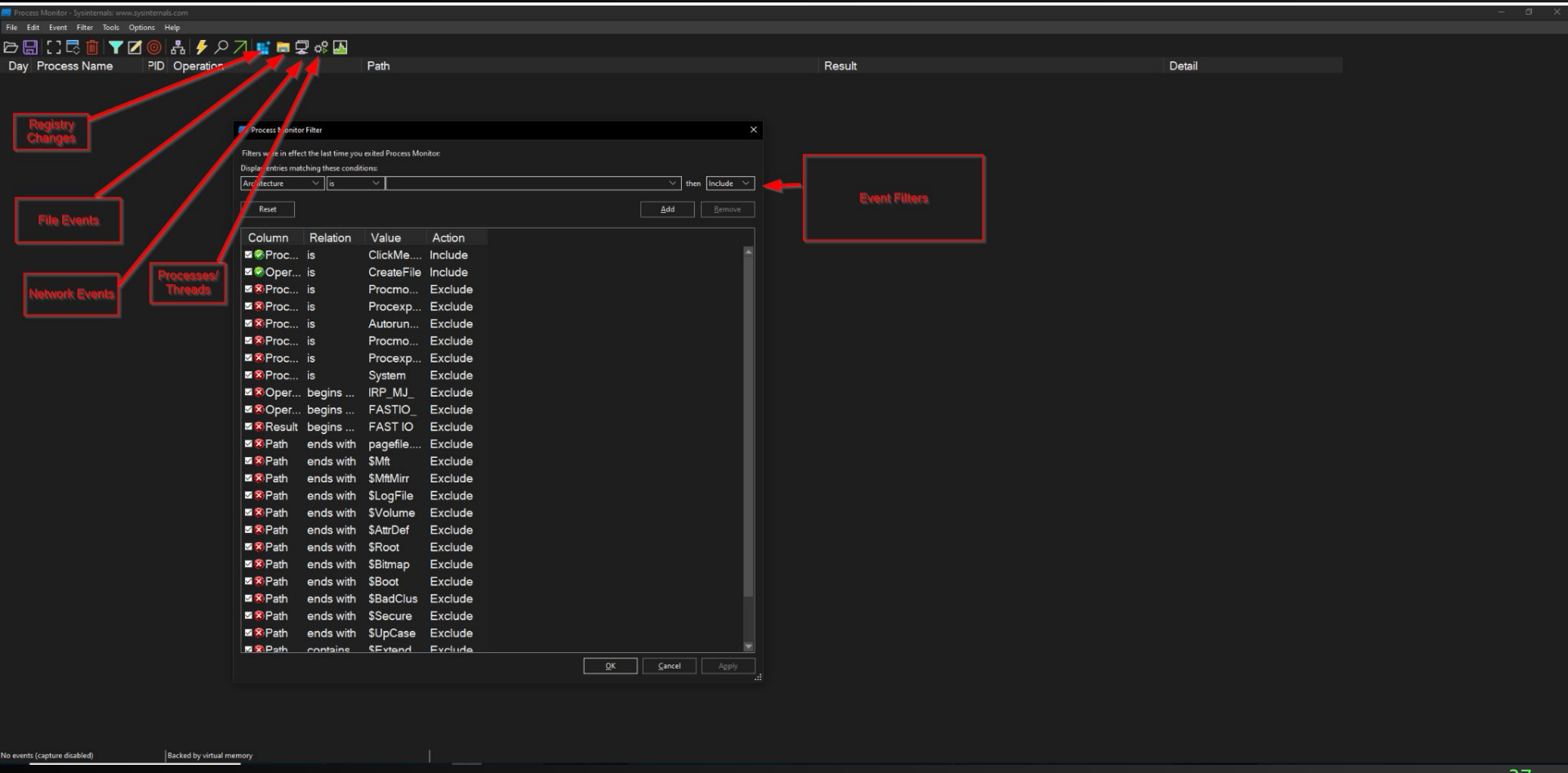
Demo:
Reading a file
C, C++, Modern c++

File IO/ Writing

Let’s figure it out together!

Procmon: Looking at File operations

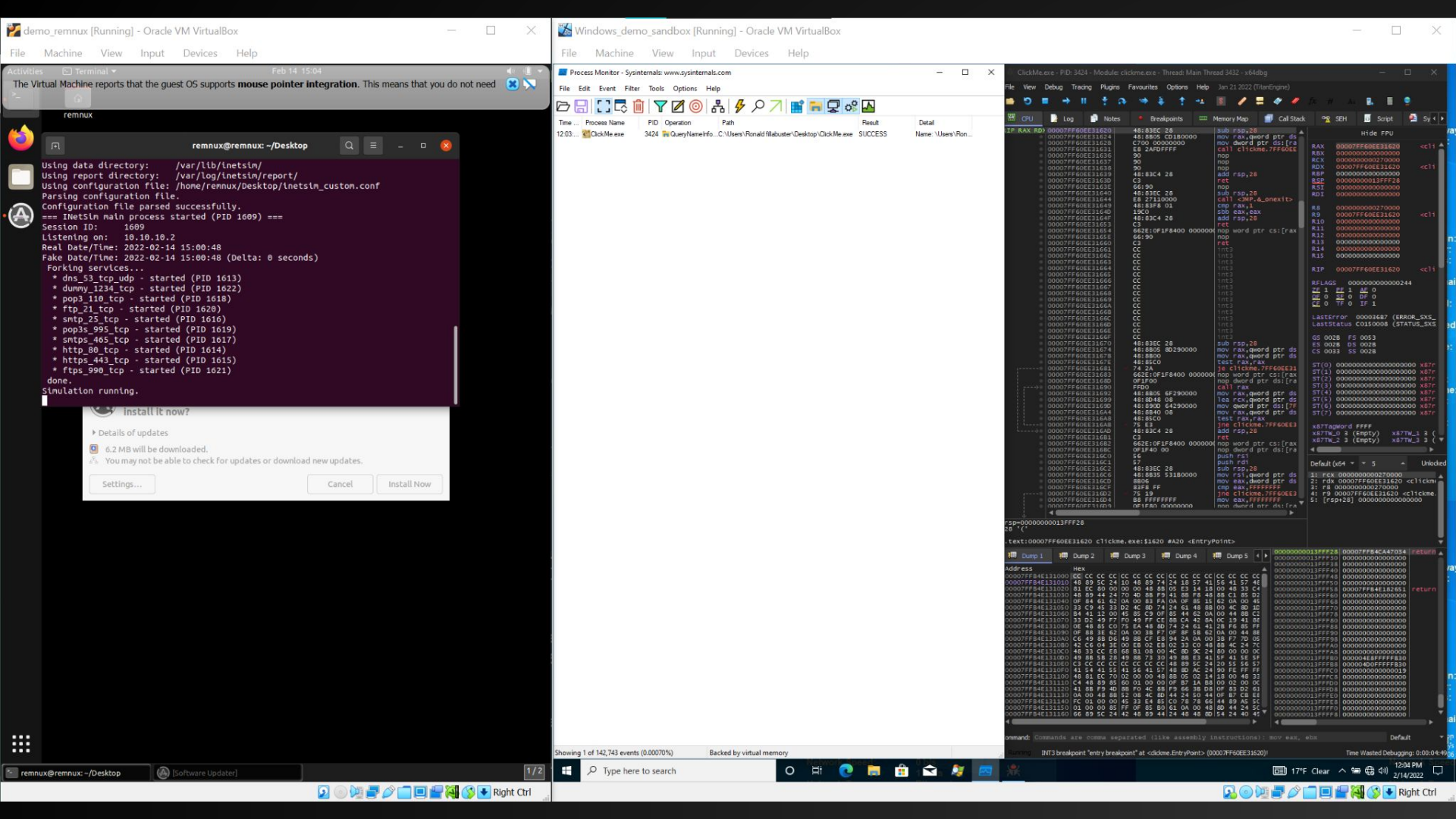
- Monitoring tool for Windows
- Displays shows real-time file system, Registry, network and process/thread activity.
- Also provides Image load information, meaning if a binary uses Explicit Dynamic LInking, we can see it load the DLL using only Procmon.
- Procmon is an incredibly powerful tool– so much so– that a lot of malware will look for the presence of Procmon running as an anti-debugging tactic

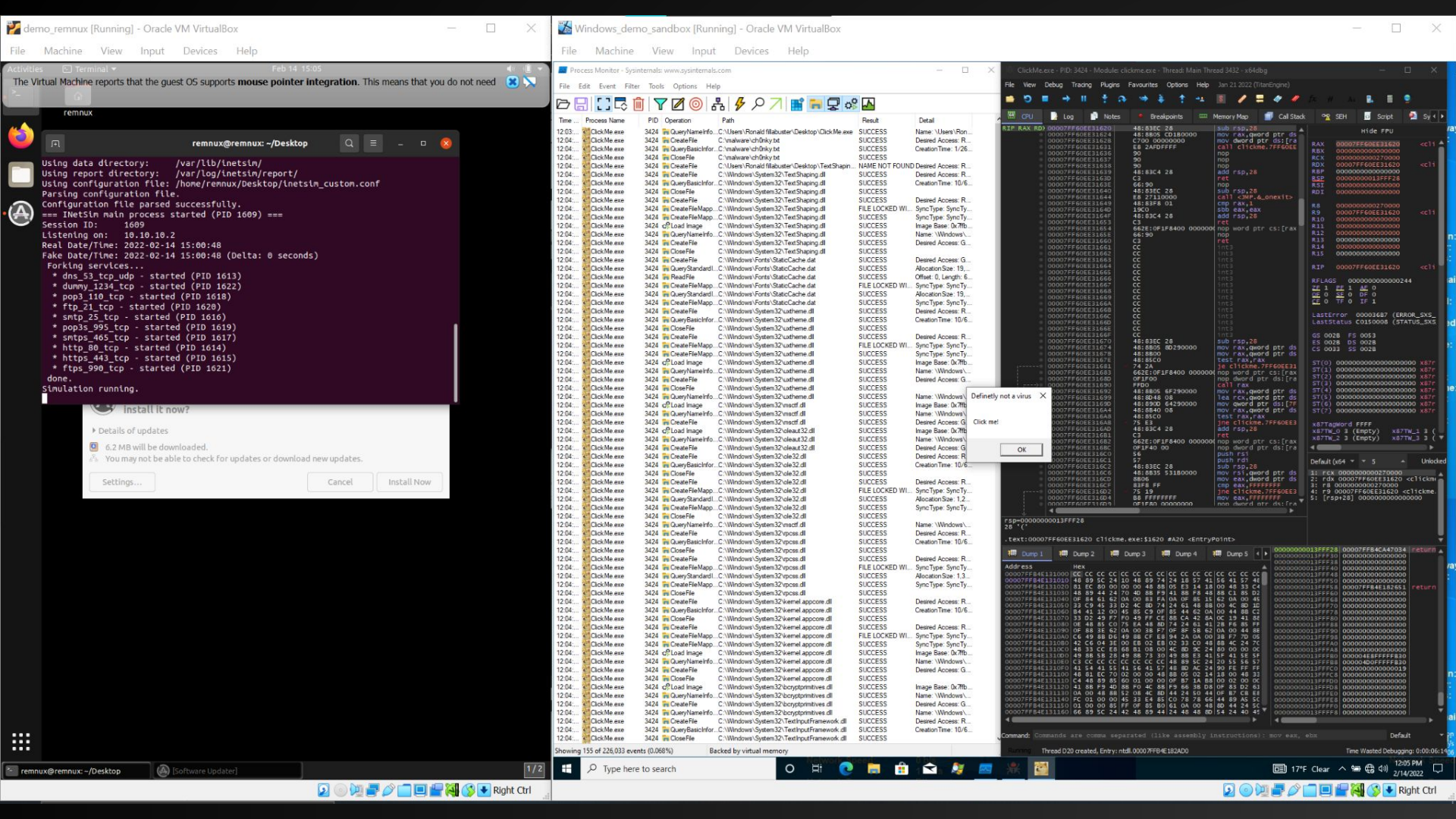

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Day Process Name PID Operation Path Result Detail
Registry Changes
File Events
Network Events
Processes/ Threads
Process Monitor Filter
Filters were in effect the last time you exited Process Monitor:
Display entries matching these conditions:
Architecture is then Include
Reset Add Remove
Column Relation Value Action
Proc... is ClickMe.... Include
Oper... is CreateFile Include
Proc... is Procmo... Exclude
Proc... is Procexp... Exclude
Proc... is Autorun... Exclude
Proc... is Procmo... Exclude
Proc... is Procexp... Exclude
Proc... is System Exclude
Oper... begins ... IRP_MJ_ Exclude
Oper... begins ... FASTIO_ Exclude
Result begins ... FAST IO Exclude
Path ends with pagefile.... Exclude
Path ends with $Mft Exclude
Path ends with $MftMirr Exclude
Path ends with $LogFile Exclude
Path ends with $Volume Exclude
Path ends with $AttrDef Exclude
Path ends with $Root Exclude
Path ends with $Bitmap Exclude
Path ends with $Boot Exclude
Path ends with $BadClus Exclude
Path ends with $Secure Exclude
Path ends with $UpCase Exclude
OK Cancel Apply
Event Filters
No events (capture disabled)
Backed by virtual memory

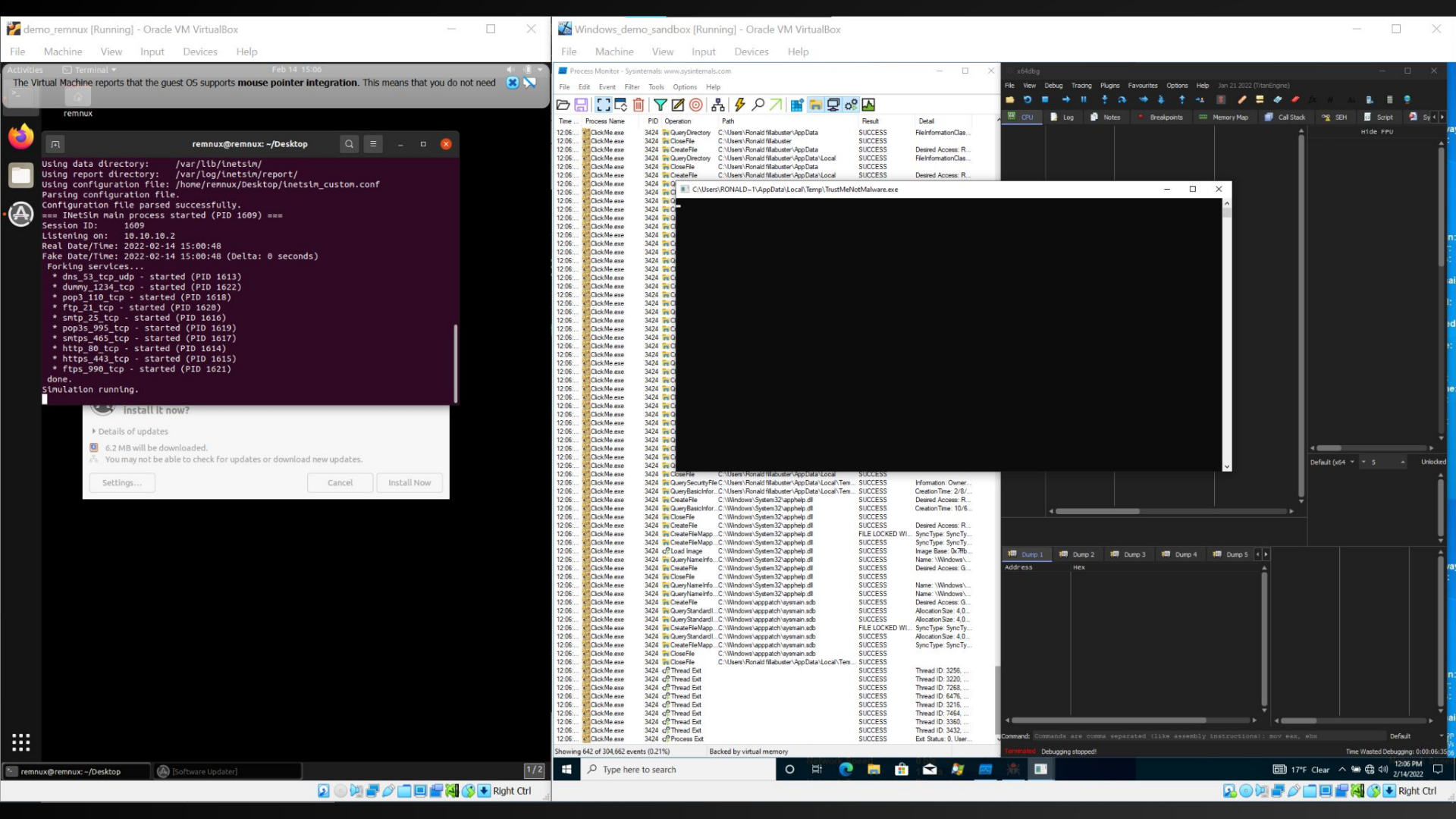
Demo
Using Procmon on ClickMe.exe

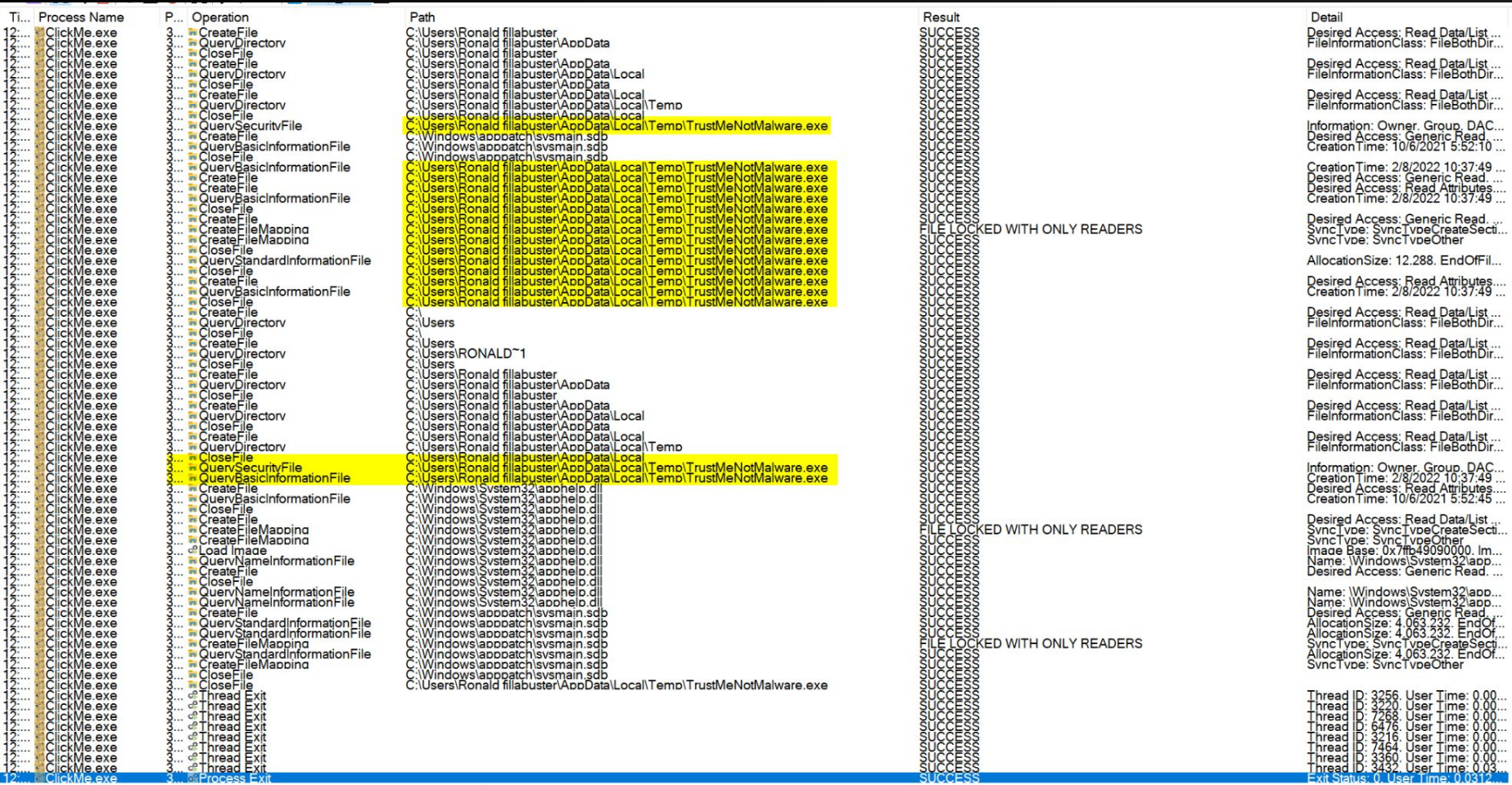
Filters for File IO

- Start Procmon and turn off live capture
- Start ClickMe.exe via x64dbg
- Set a filter for Proc name is ClickMe.exe
- Disable Registry, network and processes information
- Make sure File events are enabled
- BP sleep, set RCX=0
- Enable capture
- Run the binary
- Observe the calls to `CreateFile`
- Alternatively, `bp CreateFileA` in x64dbg


demo_remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 14 15:04
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need
remnux
remnux@remnux: ~/Desktop
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /home/remnux/Desktop/inetsim_custom.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1609) ===
Session ID: 1609
Listening on: 10.10.10.2
Real Date/Time: 2022-02-14 15:00:48
Fake Date/Time: 2022-02-14 15:00:48 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1613)
* dummy_1234_tcp - started (PID 1622)
* pop3_110_tcp - started (PID 1618)
* ftp_21_tcp - started (PID 1620)
* smtp_25_tcp - started (PID 1616)
* pop3s_995_tcp - started (PID 1619)
* smtps_465_tcp - started (PID 1617)
* http_80_tcp - started (PID 1614)
* https_443_tcp - started (PID 1615)
* ftps_990_tcp - started (PID 1621)
done.
Simulation running.
Install it now?
Details of updates
6.2 MB will be downloaded.
You may not be able to check for updates or download new updates.
Settings...
Cancel
Install Now
remnux@remnux: ~/Desktop
[Software Updater]
1 / 2
Right Ctrl
Windows_demo_sandbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
12:03:... ClickMe.exe 3424 QueryNameInfo... C:\Users\Ronald fillabuster\Desktop\ClickMe.exe SUCCESS Name: \Users\Ron...
Showing 1 of 142,743 events (0.00070%) Backed by virtual memory
ClickMe.exe - PID: 3424 - Module: clickme.exe - Thread: Main Thread 3432 - x64dbg
Hide FPU
RAX 00007FF60EE31620
RBX 0000000000000000
RCX 0000000000270000
RDX 00007FF60EE31620
RBP 0000000000000000
RSP 000000000013FFF28
RSI 0000000000000000
RDI 0000000000000000
R8 0000000000270000
R9 00007FF60EE31620
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF60EE31620
RFLAGS 0000000000000244
LastError 00003687 (ERROR_SXS_...
LastStatus C0150008 (STATUS_SXS...
GS 002B FS 0053
ES 002B DS 002B
CS 0033 SS 002B
Unlocked
Type here to search
17°F Clear
12:04 PM
2/14/2022
Right Ctrl

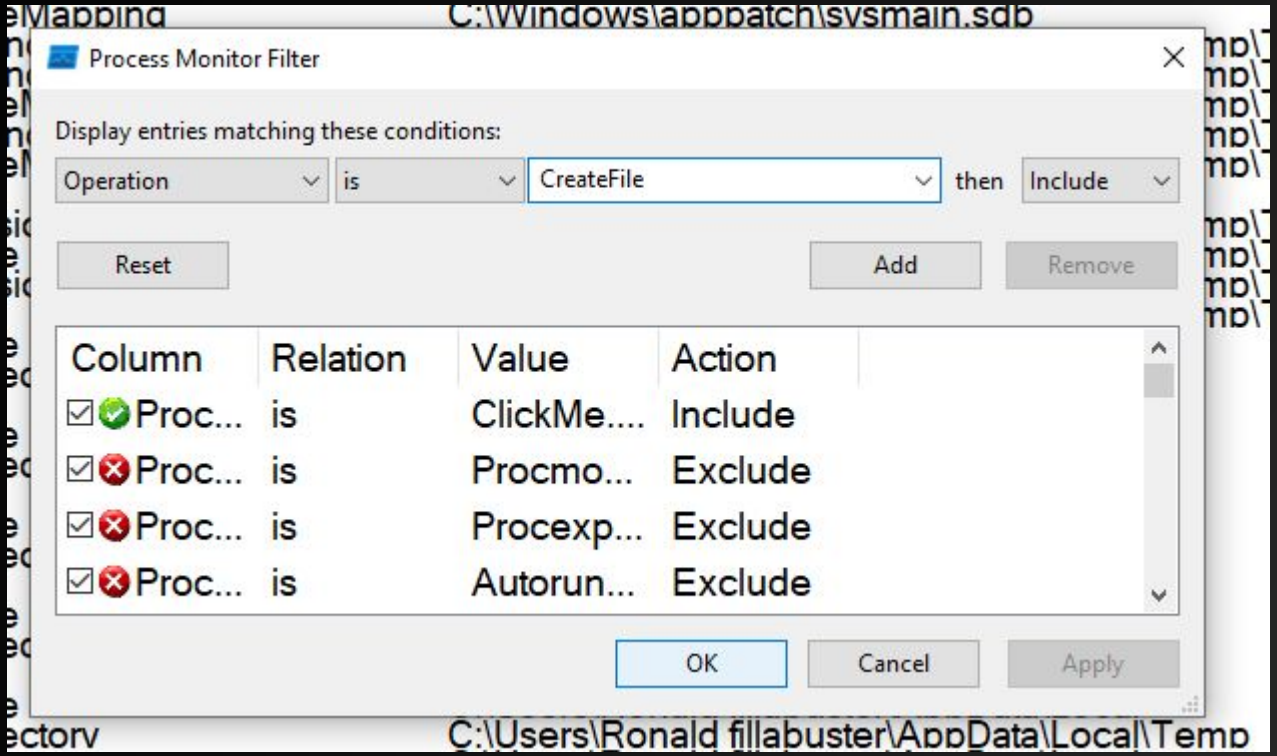

demo_remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 14 15:05
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need
remnux
remnux@remnux: ~/Desktop
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /home/remnux/Desktop/inetsim_custom.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1609) ===
Session ID: 1609
Listening on: 10.10.10.2
Real Date/Time: 2022-02-14 15:00:48
Fake Date/Time: 2022-02-14 15:00:48 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1613)
* dummy_1234_tcp - started (PID 1622)
* pop3_110_tcp - started (PID 1618)
* ftp_21_tcp - started (PID 1628)
* smtp_25_tcp - started (PID 1616)
* pop3s_995_tcp - started (PID 1619)
* smtps_465_tcp - started (PID 1617)
* http_80_tcp - started (PID 1614)
* https_443_tcp - started (PID 1615)
* ftps_990_tcp - started (PID 1621)
done.
Simulation running.
Install it now?
Details of updates
6.2 MB will be downloaded.
You may not be able to check for updates or download new updates.
Settings...
Cancel
Install Now
remnux@remnux: ~/Desktop
[Software Updater]
1 / 2
Right Ctrl
Windows_demo_sandbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Showing 155 of 226,033 events (0.068%)
Backed by virtual memory
ClickMe.exe - PID: 3424 - Module: clickme.exe - Thread: Main Thread 3432 - x64dbg
File View Debug Tracing Plugins Favourites Options Help Jan 21 2022 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Sy
Hide FPU
Definetly not a virus
Click me!
OK
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Thread 0x20 created, Entry: ntdll.00007FFB4E182AD0
Time Wasted Debugging: 0:00:06:14
Type here to search
17°F Clear
12:05 PM
2/14/2022
Right Ctrl

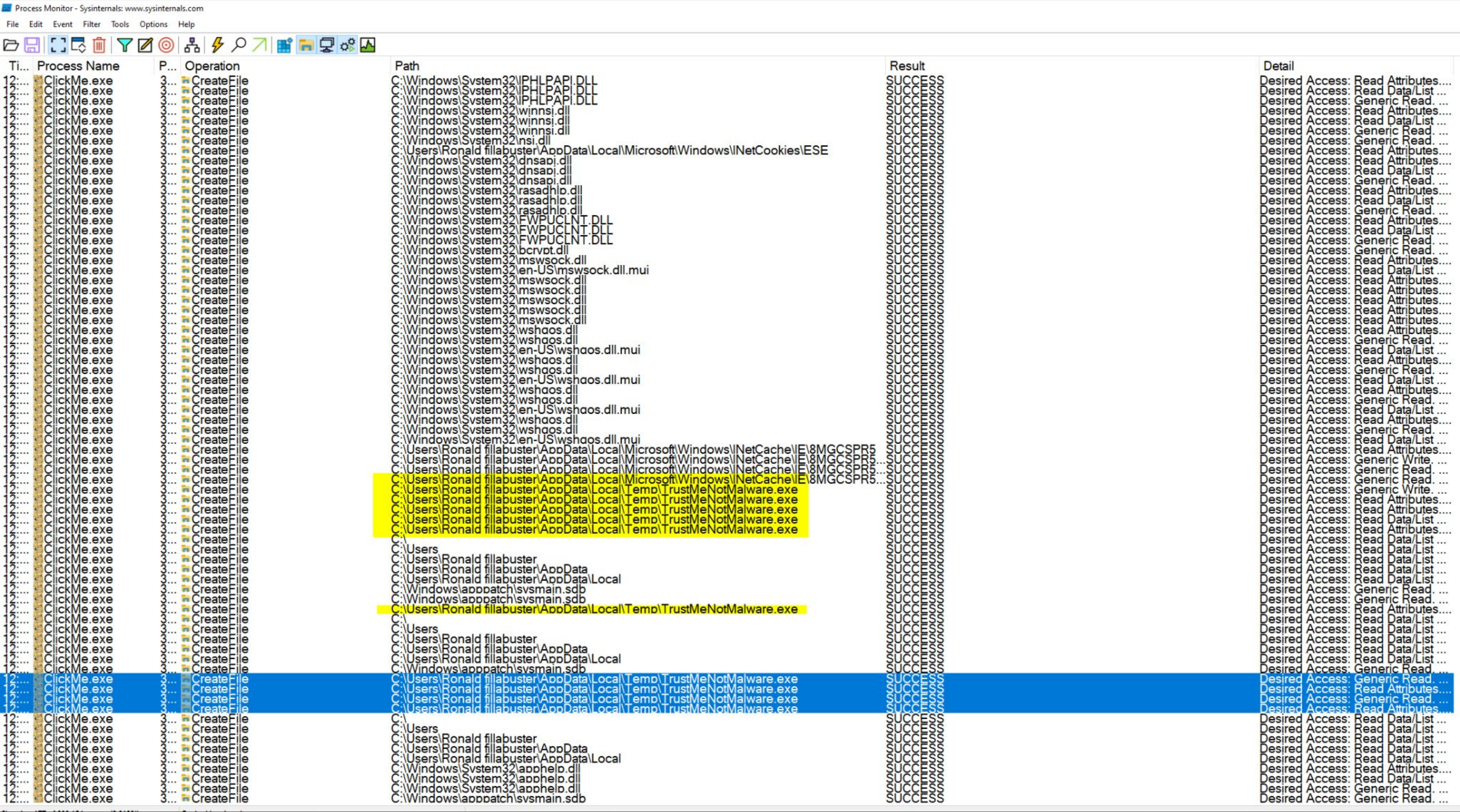

demo_remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 14 15:06
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need
remnux
remnux@remnux: ~/Desktop
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /home/remnux/Desktop/inetsim_custom.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1609) ===
Session ID: 1609
Listening on: 10.10.10.2
Real Date/Time: 2022-02-14 15:00:48
Fake Date/Time: 2022-02-14 15:00:48 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1613)
* dummy_1234_tcp - started (PID 1622)
* pop3_110_tcp - started (PID 1618)
* ftp_21_tcp - started (PID 1620)
* smtp_25_tcp - started (PID 1616)
* pop3s_995_tcp - started (PID 1619)
* smtps_465_tcp - started (PID 1617)
* http_80_tcp - started (PID 1614)
* https_443_tcp - started (PID 1615)
* ftps_990_tcp - started (PID 1621)
done.
Simulation running.
Install it now?
Details of updates
6.2 MB will be downloaded.
You may not be able to check for updates or download new updates.
Settings...
Cancel
Install Now
remnux@remnux: ~/Desktop
[Software Updater]
1 / 2
Right Ctrl
Windows_demo_sandbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
C:\Users\RONALD~1\AppData\Local\Temp\TrustMeNotMalware.exe
x64dbg
File View Debug Tracing Plugins Favourites Options Help
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5
Address Hex
Command:
Terminated Debugging stopped!
Showing 642 of 304,662 events (0.21%) Backed by virtual memory
Type here to search
17°F Clear
12:06 PM
2/14/2022
Right Ctrl



Ti...	Process Name	P...	Operation	Path	Result	Detail
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\Ronald fillabuster\AppData	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\Ronald fillabuster\AppData\Local\Temp	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	
12:...	ClickMe.exe	3...	QuerySecurityFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Information: Owner, Group, DAC...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, ...
12:...	ClickMe.exe	3...	QueryBasicInformationFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	CreationTime: 10/6/2021 5:52:10 ...
12:...	ClickMe.exe	3...	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
12:...	ClickMe.exe	3...	QueryBasicInformationFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	CreationTime: 2/8/2022 10:37:49 ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Generic Read, ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes, ...
12:...	ClickMe.exe	3...	QueryBasicInformationFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	CreationTime: 2/8/2022 10:37:49 ...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Generic Read, ...
12:...	ClickMe.exe	3...	CreateFileMapping	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSecti...
12:...	ClickMe.exe	3...	CreateFileMapping	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	SyncType: SyncTypeOther
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	
12:...	ClickMe.exe	3...	QueryStandardInformationFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	AllocationSize: 12.288, EndOfFil...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes, ...
12:...	ClickMe.exe	3...	QueryBasicInformationFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	CreationTime: 2/8/2022 10:37:49 ...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\RONALD~1	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\Ronald fillabuster\AppData	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	QueryDirectory	C:\Users\Ronald fillabuster\AppData\Local\Temp	SUCCESS	FileInformationClass: FileBothDir...
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	
12:...	ClickMe.exe	3...	QuerySecurityFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Information: Owner, Group, DAC...
12:...	ClickMe.exe	3...	QueryBasicInformationFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	CreationTime: 2/8/2022 10:37:49 ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: Read Attributes, ...
12:...	ClickMe.exe	3...	QueryBasicInformationFile	C:\Windows\System32\apphelp.dll	SUCCESS	CreationTime: 10/6/2021 5:52:45 ...
12:...	ClickMe.exe	3...	CloseFile	C:\Windows\System32\apphelp.dll	SUCCESS	
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFileMapping	C:\Windows\System32\apphelp.dll	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSecti...
12:...	ClickMe.exe	3...	CreateFileMapping	C:\Windows\System32\apphelp.dll	SUCCESS	SyncType: SyncTypeOther
12:...	ClickMe.exe	3...	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS	Image Base: 0x7ffb49090000, Im...
12:...	ClickMe.exe	3...	QueryNameInformationFile	C:\Windows\System32\apphelp.dll	SUCCESS	Name: \Windows\System32\app...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: Generic Read, ...
12:...	ClickMe.exe	3...	CloseFile	C:\Windows\System32\apphelp.dll	SUCCESS	
12:...	ClickMe.exe	3...	QueryNameInformationFile	C:\Windows\System32\apphelp.dll	SUCCESS	Name: \Windows\System32\app...
12:...	ClickMe.exe	3...	QueryNameInformationFile	C:\Windows\System32\apphelp.dll	SUCCESS	Name: \Windows\System32\app...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, ...
12:...	ClickMe.exe	3...	QueryStandardInformationFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,063,232, EndOf...
12:...	ClickMe.exe	3...	QueryStandardInformationFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,063,232, EndOf...
12:...	ClickMe.exe	3...	CreateFileMapping	C:\Windows\apppatch\sysmain.sdb	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSecti...
12:...	ClickMe.exe	3...	QueryStandardInformationFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,063,232, EndOf...
12:...	ClickMe.exe	3...	CreateFileMapping	C:\Windows\apppatch\sysmain.sdb	SUCCESS	SyncType: SyncTypeOther
12:...	ClickMe.exe	3...	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
12:...	ClickMe.exe	3...	CloseFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 3256, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 3220, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 7268, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 6476, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 3216, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 7464, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 3360, User Time: 0.00...
12:...	ClickMe.exe	3...	Thread Exit		SUCCESS	Thread ID: 3432, User Time: 0.03...
12:...	ClickMe.exe	3...	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0312...

Filtering by Operation





Ti...	Process Name	P...	Operation	Path	Result	Detail
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\IPHLPAPI.DLL	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\winnsi.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\winnsi.dll	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\winnsi.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\nsi.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Microsoft\Windows\INetCookies\ESE	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\dnsapi.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\dnsapi.dll	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\dnsapi.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\rasadhlp.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\rasadhlp.dll	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\rasadhlp.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\FWPUCLNT.DLL	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\FWPUCLNT.DLL	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\FWPUCLNT.DLL	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\bcrypt.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\mswsock.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\en-US\mswsock.dll.mui	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\mswsock.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\mswsock.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\mswsock.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\mswsock.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\mswsock.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\en-US\wshqos.dll.mui	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\en-US\wshqos.dll.mui	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\en-US\wshqos.dll.mui	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\en-US\wshqos.dll.mui	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Microsoft\Windows\INetCache\IE\8MGCSPR5	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Microsoft\Windows\INetCache\IE\8MGCSPR5...	SUCCESS	Desired Access: Generic Write. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Microsoft\Windows\INetCache\IE\8MGCSPR5...	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Microsoft\Windows\INetCache\IE\8MGCSPR5...	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Generic Write. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local\Temp\TrustMeNotMalware.exe	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Users\Ronald fillabuster\AppData\Local	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: Read Attributes....
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: Read Data/List ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: Generic Read. ...
12:...	ClickMe.exe	3...	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read. ...

Procmon File tips

- Procmon displays a LOT of information when no filters are applied
- Many organizations will install Sysmon– a system wide implementation of Procmon that will send all of the events to an analysis environment
- For us, it is best to run a processes via x64dbg, turn off capture, and set filters for the target processes, enable capture then run
- Once the processes is done/we are happy with the execution, we can search through the mountain of data created
- I usually start with all `CreateFile` calls, as they can give information about loaded DLLs, files opened/created

Discussion:

Files!