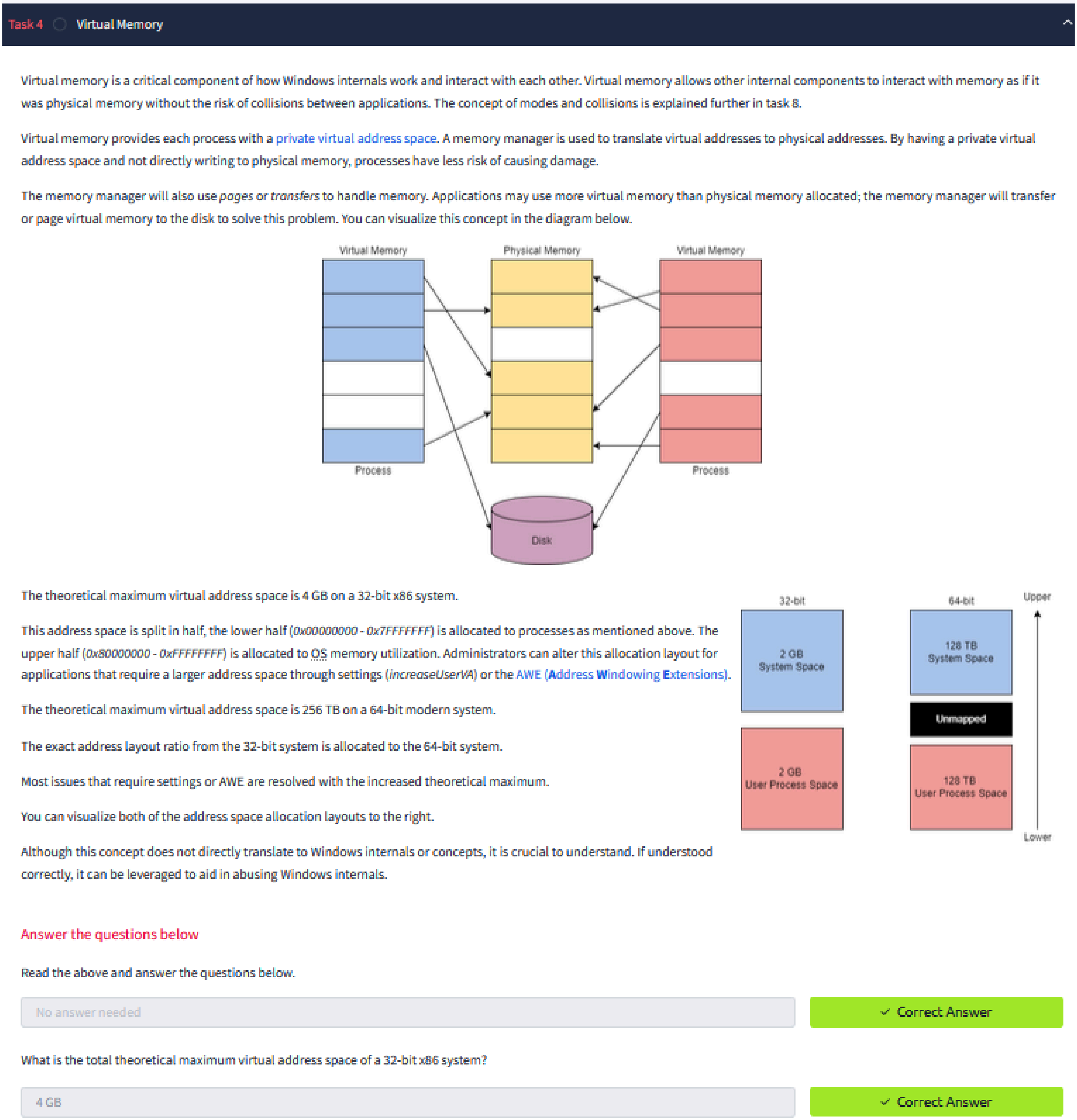
2 - Virtual Memory



Virtual memory is a critical component of how Windows internals work and interact with each other. Virtual memory allows other internal components to interact with memory as if it was physical memory without the risk of collisions between applications. The concept of modes and collisions is explained further in task 8.

Virtual memory provides each process with a private virtual address space. A memory manager is used to translate virtual addresses to physical addresses. By having a private virtual address space and not directly writing to physical memory, processes have less risk of causing damage.

The memory manager will also use *pages* or *transfers* to handle memory. Applications may use more virtual memory than physical memory allocated; the memory manager will transfer or page virtual memory to the disk to solve this problem. You can visualize this concept in the diagram below.

The theoretical maximum virtual address space is 4 GB on a 32-bit x86 system.

This address space is split in half, the lower half (*0x00000000 - 0x7FFFFFFF*) is allocated to processes as mentioned above. The upper half (*0x80000000 - 0xFFFFFFFF*) is allocated to OS memory utilization. Administrators can alter this allocation layout for applications that require a larger address space through settings (*increaseUserVA*) or the AWE (**A**ddress **W**indowing **E**xtensions).

The theoretical maximum virtual address space is 256 TB on a 64-bit modern system.

The exact address layout ratio from the 32-bit system is allocated to the 64-bit system.

Most issues that require settings or AWE are resolved with the increased theoretical maximum.

You can visualize both of the address space layouts to the right.

Although this concept does not directly translate to Windows internals or concepts, it is crucial to understand. If understood correctly, it can be leveraged to aid in abusing Windows internals.

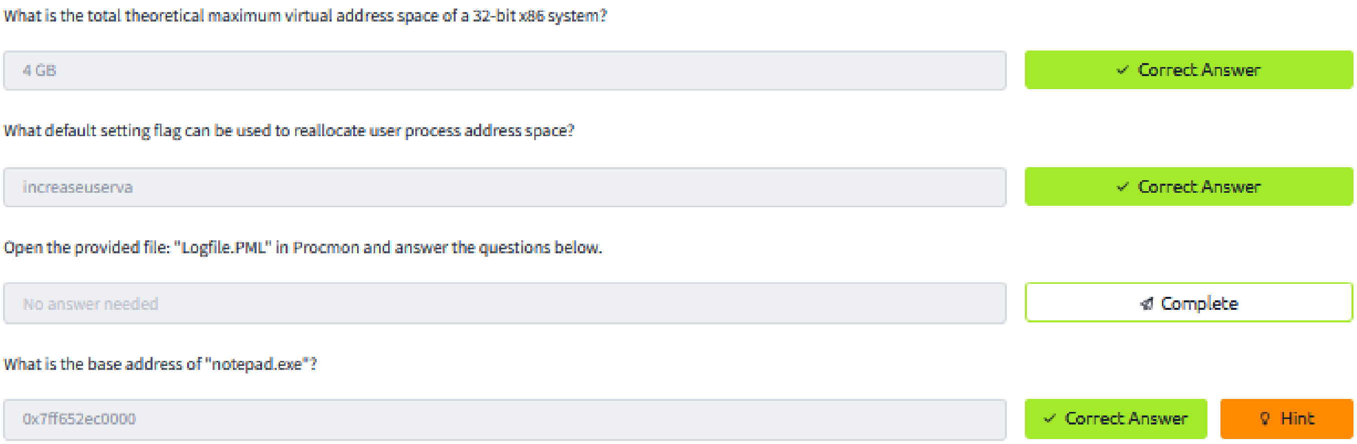
Answer the questions below

Read the above and answer the questions below.

No answer needed

What is the total theoretical maximum virtual address space of a 32-bit x86 system?

4 GB



What is the total theoretical maximum virtual address space of a 32-bit x86 system?

4 GB

✓ Correct Answer

What default setting flag can be used to reallocate user process address space?

increaseuserva

✓ Correct Answer

Open the provided file: "Logfile.PML" in Procmon and answer the questions below.

No answer needed

Complete

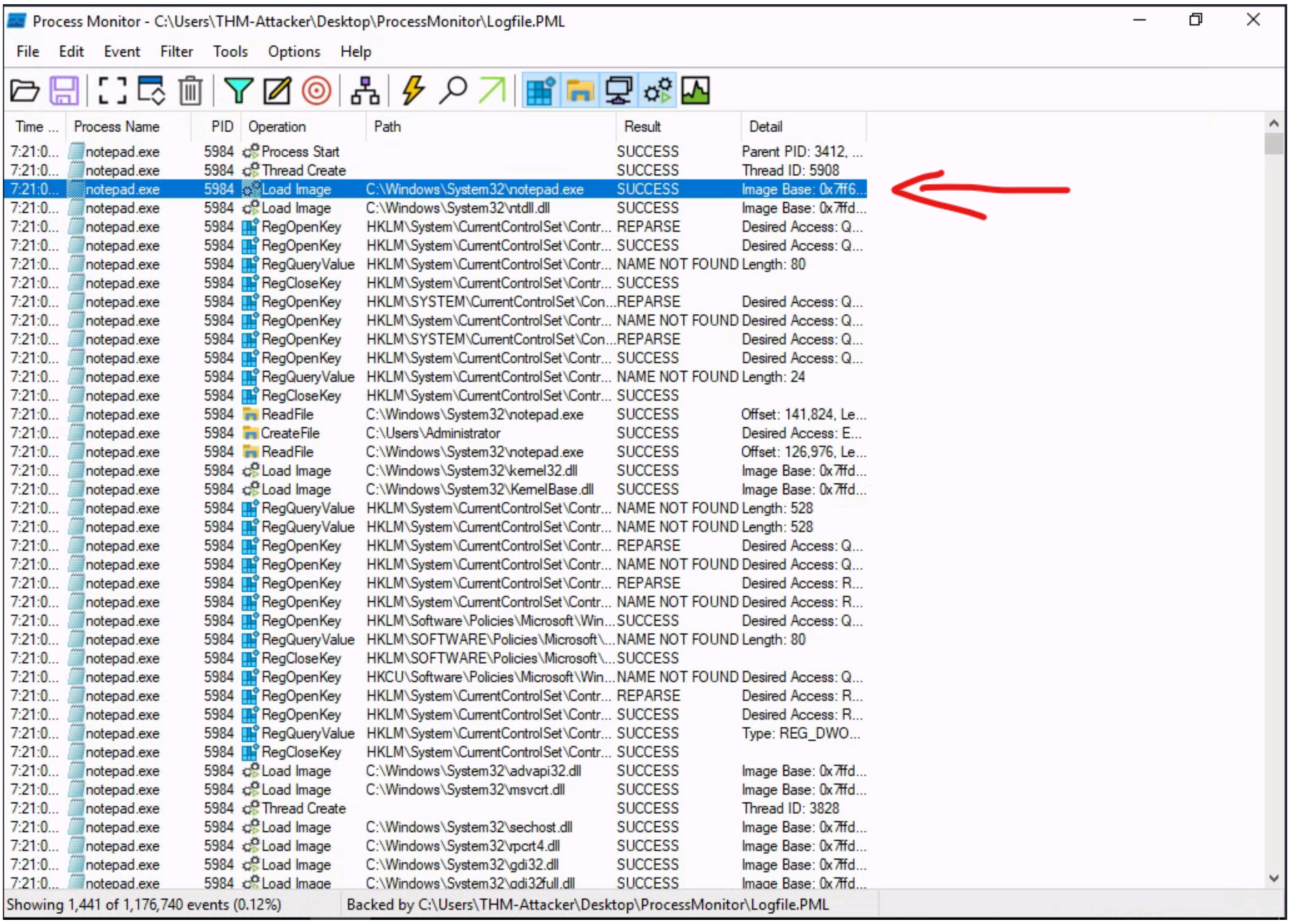
What is the base address of "notepad.exe"?

0x7ff652ec0000

✓ Correct Answer

Hint

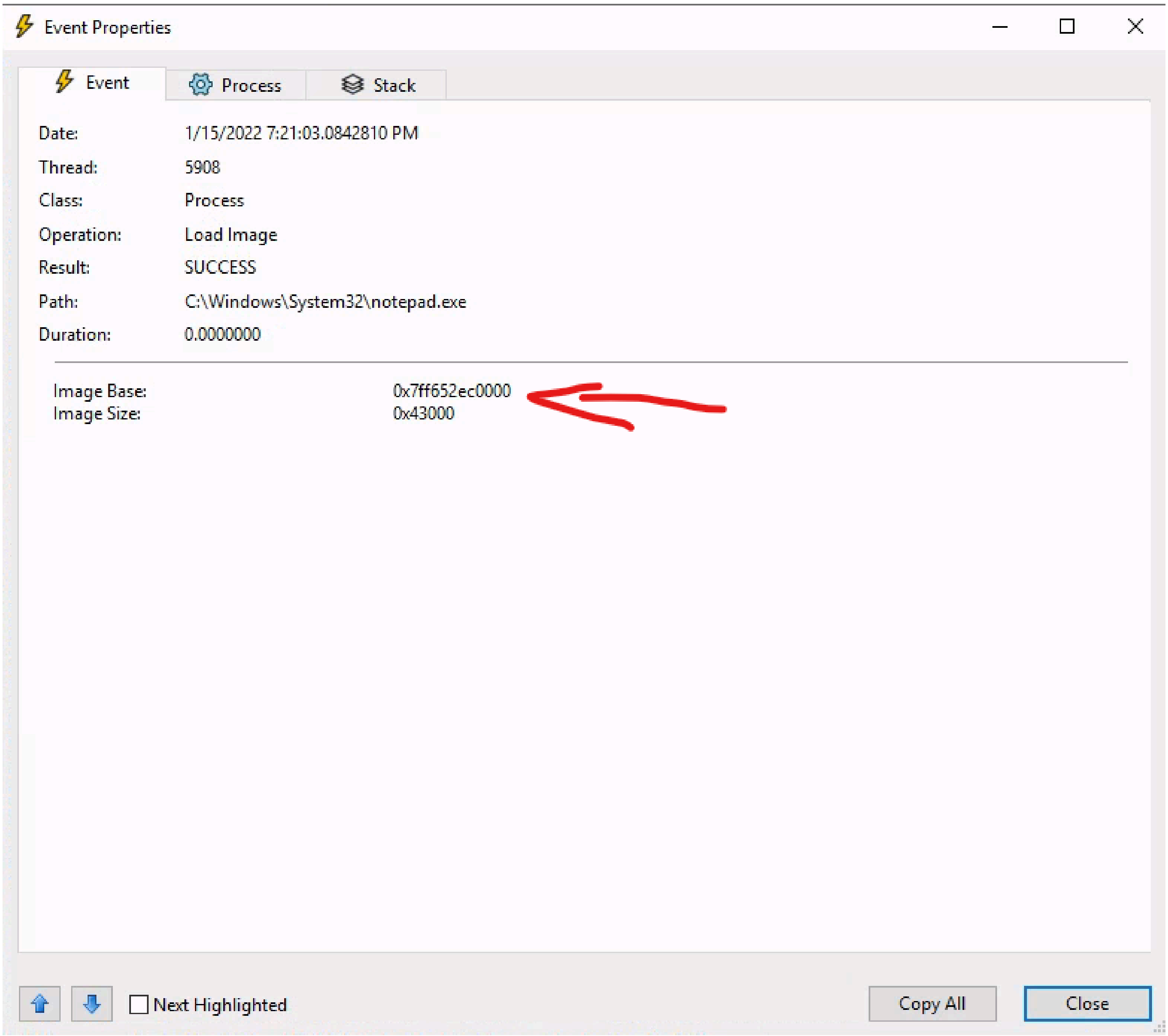
To answer the last questions, we need to go through the threads, and find the first one where the operations is "Load Image", and the address is going to be listed in there. We can find it in the Image Base entry in the Event tab, or in the Process tab under Modules.



Process Monitor - C:\Users\THM-Attacker\Desktop\ProcessMonitor\Logfile.PML
File
Edit
Event
Filter
Tools
Options
Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
7:21:0...	notepad.exe	5984	Process Start		SUCCESS	Parent PID: 3412, ...
7:21:0...	notepad.exe	5984	Thread Create		SUCCESS	Thread ID: 5908
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\notepad.exe	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 141,824, Le...
7:21:0...	notepad.exe	5984	CreateFile	C:\Users\Administrator	SUCCESS	Desired Access: E...
7:21:0...	notepad.exe	5984	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 126,976, Le...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
7:21:0...	notepad.exe	5984	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Thread Create		SUCCESS	Thread ID: 3828
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffd...

Showing 1,441 of 1,176,740 events (0.12%) | Backed by C:\Users\THM-Attacker\Desktop\ProcessMonitor\Logfile.PML



Date: 1/15/2022 7:21:03.0842810 PM

Thread: 5908

Class: Process

Operation: Load Image

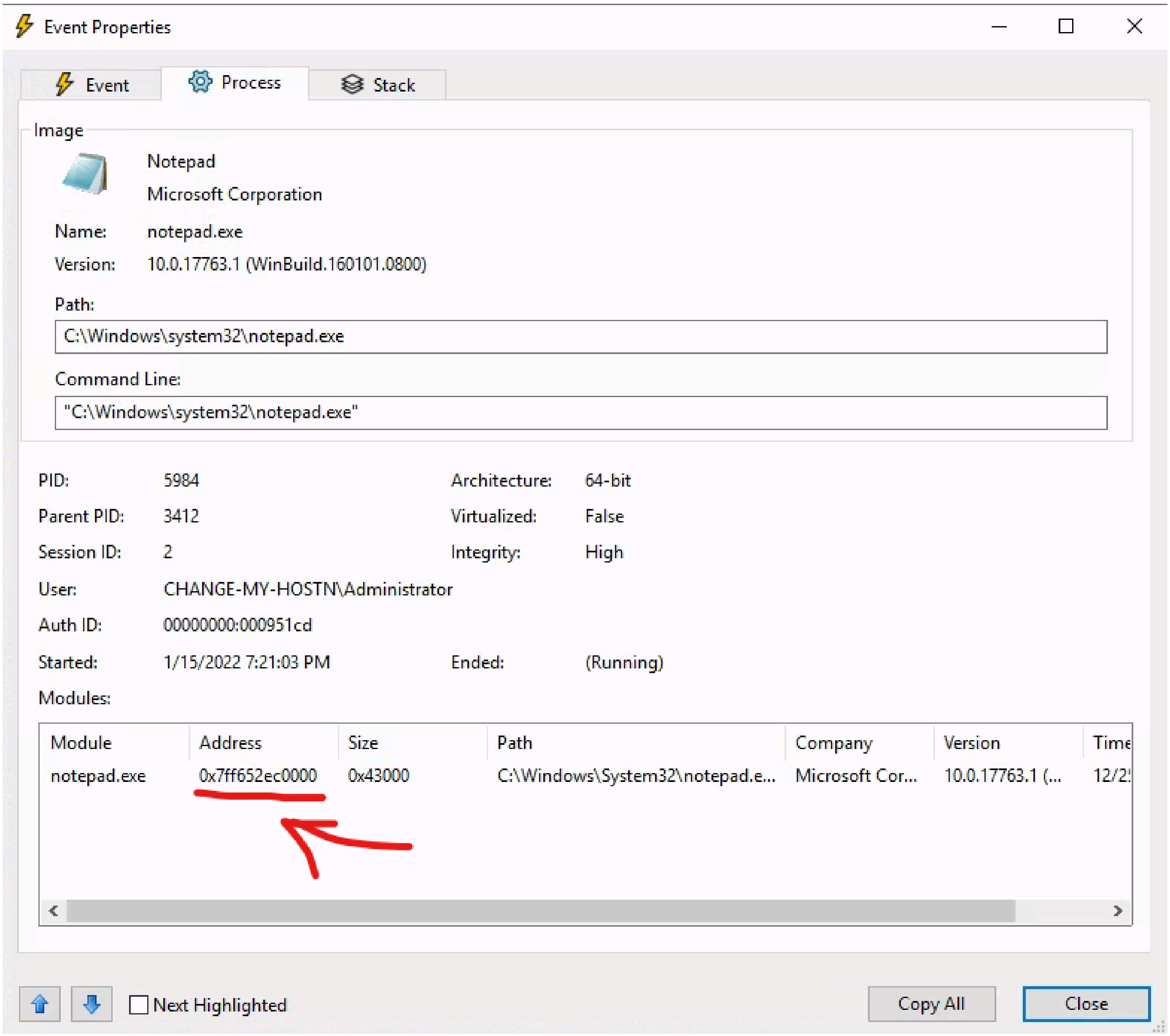
Result: SUCCESS

Path: C:\Windows\System32\notepad.exe

Duration: 0.0000000

Image Base: 0x7ff652ec0000

Image Size: 0x43000



Image

Notepad
Microsoft Corporation

Name: notepad.exe
Version: 10.0.17763.1 (WinBuild.160101.0800)

Path:
C:\Windows\system32\notepad.exe

Command Line:
"C:\Windows\system32\notepad.exe"

PID: 5984
Architecture: 64-bit
Parent PID: 3412
Virtualized: False
Session ID: 2
Integrity: High
User: CHANGE-MY-HOSTN\Administrator
Auth ID: 00000000:000951cd
Started: 1/15/2022 7:21:03 PM
Ended: (Running)

Modules:

Module	Address	Size	Path	Company	Version	Time
notepad.exe	0x7ff652ec0000	0x43000	C:\Windows\System32\notepad.e...	Microsoft Cor...	10.0.17763.1 (...	12/2!

I think we can only see the base address in the third thread is because the process was yet to be assigned a base address until so. Maybe that is normal behavior of this process in specific. Not sure.