Toan Ngo
Date:3/6/24

Lap 7 report: crash dump file

As we start this report we gotta ask ourselves what is a dump file on an operating system? Why are dumps files important ? and how many dump file types there are in the window operating system. This is what we will be driving into today.

First question: what are the dump files on an operating system and why are they important ? dumps files are the files that contain all related information about your operating system at the time that file is dumped, and usually it will dump at this particular location [%SystemRoot%\MEMORY.DMP]. What dumps files are responsible for is to write the current state of the machine including what type of error that the operating system has encountered in the files so that other people can investigate what happened to that machine just by reading the dumps files. Also the dumps files get generated when your operating system crashes, which you can use to investigate the reason for that crash at a later date. In the investigating world's dumps, files could serve as evidence for the operating system investigator because all the activity and the system information were written alongside with each other in the dump files which could capture what the suspect was doing with their computer at the time of the crime and could potentially lead to them getting arrested. As we can see dumps files serve a very importance function and that is to stored the current stage of the machine in a files including error,and sometime you can also create a memory dump which stored the current state memory in the files which later you can use it to investigate what happened in the memory or what causing the operating system crash. Just to imagine that dump files don't exist, then you will have no way to recover your operating system and if the system were to fail, you will have no way to investigate what/why the operating system failing because all that information is what the dump function stored in the dump files when your system experiences those crashing/ error events.

Second question: What are the different types of dump functions/types ? So in total there are 4 types of dump functions , and those are crash/automatic dump,kernel dump,small/full memory dump,and active dump. We're gonna learn a little bit about them in this lap before we move on, so let's get started with kernel dump.

Toan Ngo
Date:3/6/24

Kernel dump is the output of all kernel memory in the time of your computer crash and because of it relatively small size in comparison to full memory dump, it can be considered the most useful crash dump because it only omits those portions of memory that are unlikely to have been involved in the crash, and it relative small size is cause by not including unallocated memory, or any memory allocated to user-mode applications. you can imagine this file only contains the kernel information and nothing else and its default dumping location is in %SystemRoot%\Memory.dmp.

Small/full memory dump(complete memory dump) is a self explanatory dumping type, small memory dump can only output a small and limited amount of information about the memory, while full full dump contains full information about the memory during the time that this dump got executed.for small dump it locate in %SystemRoot%\Minidump, and for complete/ full dump they are located in %SystemRoot%\Memory.dmp respectively.

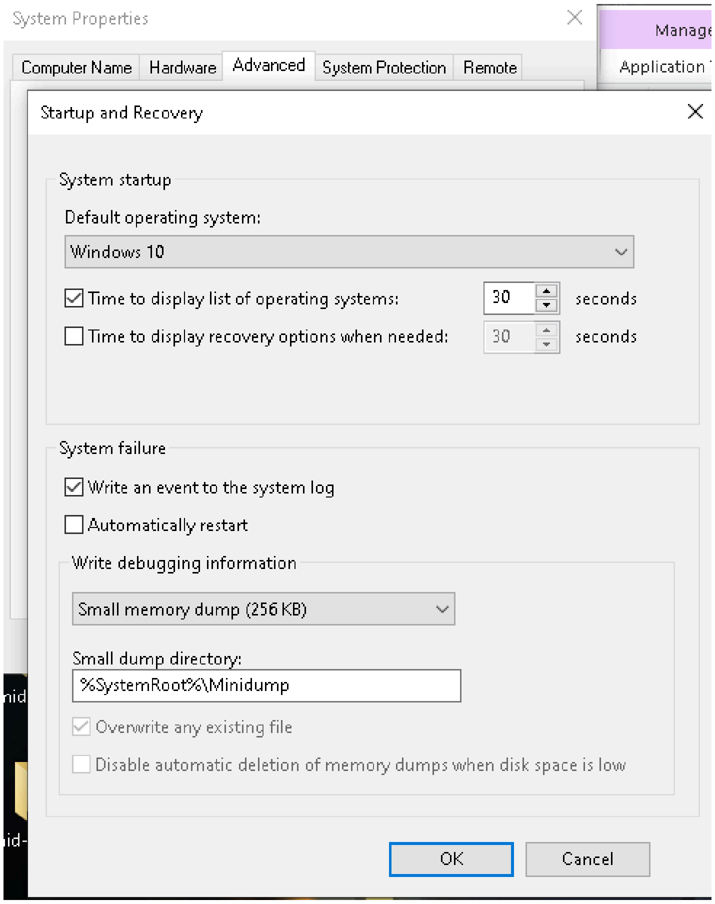
Crash dump(automatically dump) this act similar to the kernel dump but with the exception of the size of the system paging file. During the event of your window crashes, the operating system increases the size of the paging file to at least the size of RAM just to capture whatever the kernel Memory Dump exits, in contrast to kernel dump where it was set to automatically resize the memory space for the kernel dump which result in the paging size less than the ram. And for your information the files for kernel dump are located in HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\LastCrashTime after the crash dump has finished running and the file of the crash dump also stored in %SystemRoot%\Memory.dmp.

For the final dump we have the active dump. Active dump acts and behaves similar to full memory dump but with the exception of active dump comes with a filter system that only collects relevant information for the dump, and because of this the files size of the active dump are significantly smaller than a complete memory dump.

Now that we have some kinda understanding of what dump is and its type, let's get into experiment with some files dumps of our own.

First we have to find out where your dumb file are stored

Toan Ngo
Date:3/6/24



Startup and Recovery

System startup

Default operating system: Windows 10

☑ Time to display list of operating systems: 30 seconds

□ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

□ Automatically restart

Write debugging information

Small memory dump (256 KB)

Small dump directory: %SystemRoot%\Minidump

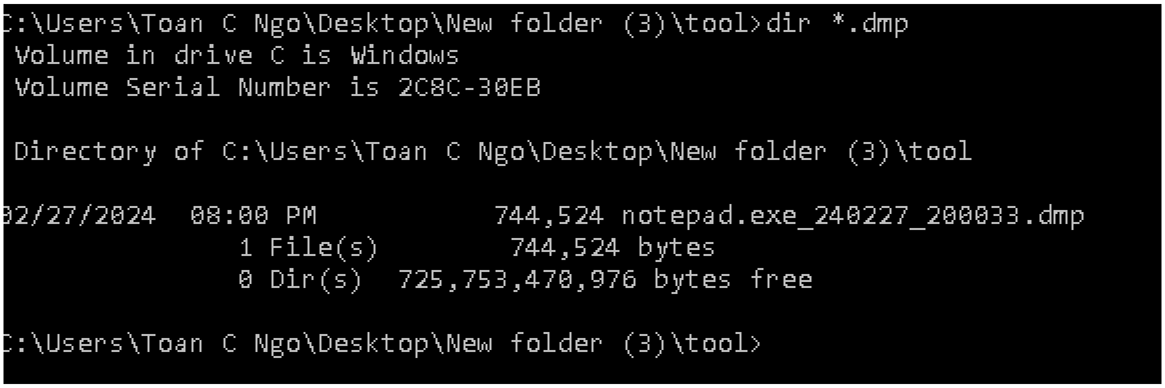
☑ Overwrite any existing file

□ Disable automatic deletion of memory dumps when disk space is low

(for my operating system my dumb files are located in systemroot/Memory, however if i were to change write debug information to mini dump, then it will automatically change the directory like in the image.)

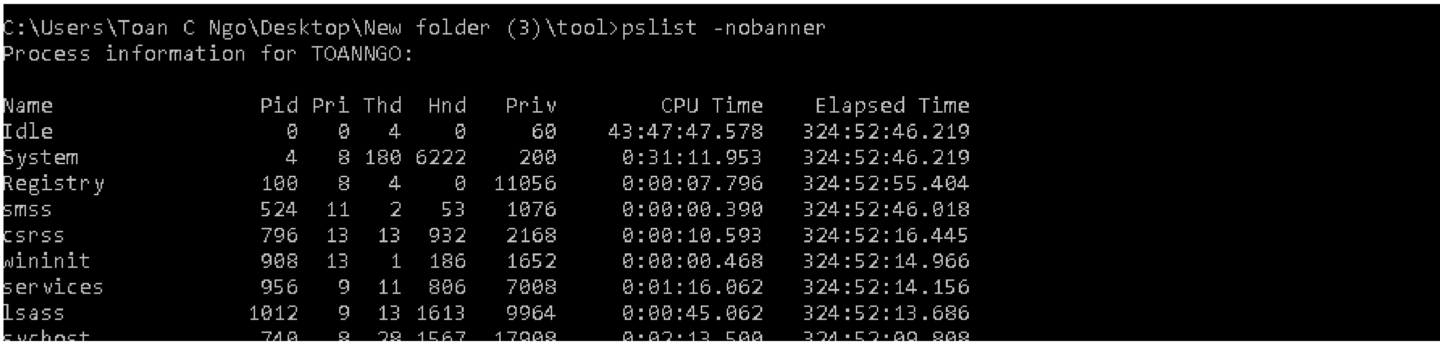
(you can access this by going to system, window key +x and select system, and on the right hand side you will see the Advanced system setting, click it then it will led you to this image.)

Toan Ngo
Date:3/6/24



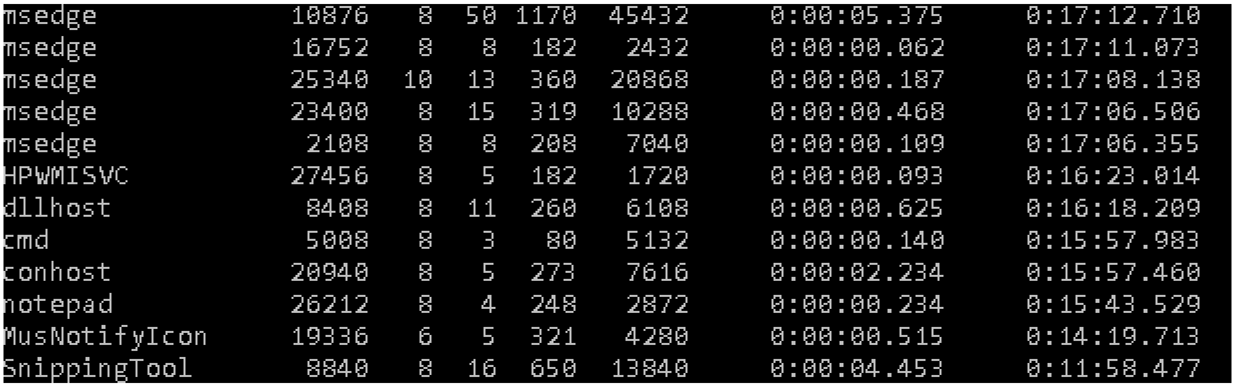
```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>dir *.dmp
 Volume in drive C is Windows
 Volume Serial Number is 2C8C-30EB

 Directory of C:\Users\Toan C Ngo\Desktop\New folder (3)\tool

02/27/2024  08:00 PM           744,524 notepad.exe_240227_200033.dmp
               1 File(s)        744,524 bytes
               0 Dir(s)  725,753,470,976 bytes free

C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>
```

(Here I was conducting a search of the current directory to see if it contain a .dmp file, and in this case it found out that i have one dump file for the application name notepad which we will learn how to do this dump later.)



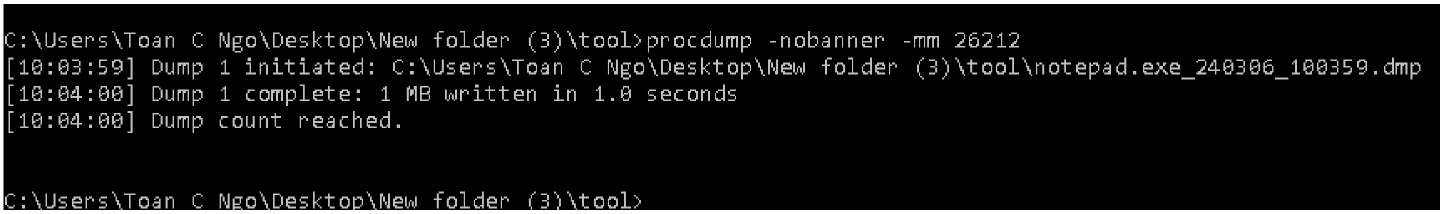
```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>pslist -nobanner
Process information for TOANNGO:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   4    0     60    43:47:47.578   324:52:46.219
System                4   8 180 6222    200     0:31:11.953   324:52:46.219
Registry            100   8   4    0  11056     0:00:07.796   324:52:55.404
smss                524  11   2   53   1076     0:00:00.390   324:52:46.018
csrss               796  13  13  932   2168     0:00:10.593   324:52:16.445
wininit             908  13   1  186   1652     0:00:00.468   324:52:14.966
services            956   9  11  806   7008     0:01:16.062   324:52:14.156
lsass              1012   9  13 1613   9964     0:00:45.062   324:52:13.686
svchost             740   8  28 1567  17908     0:02:13.500   324:52:09.808
```

(in here, what i was doing is call pslist command (process list-list a relevance process) and -nobanner (just remove the banner from the output list) which list out all the process that exist and currently open/running on my machine(note about pid, pid is a process id which we will be using in the next command, and in my case the pid for notepad is 26212))



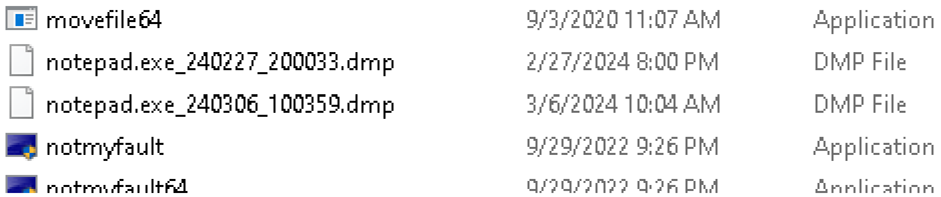
```
msedge            10876   8  50 1170  45432     0:00:05.375     0:17:12.710
msedge            16752   8   8  182   2432     0:00:00.062     0:17:11.073
msedge            25340  10  13  360  20868     0:00:00.187     0:17:08.138
msedge            23400   8  15  319  10288     0:00:00.468     0:17:06.506
msedge             2108   8   8  208   7040     0:00:00.109     0:17:06.355
HPWMISVC          27456   8   5  182   1720     0:00:00.093     0:16:23.014
dllhost            8408   8  11  260   6108     0:00:00.625     0:16:18.209
cmd                5008   8   3   80   5132     0:00:00.140     0:15:57.983
conhost           20940   8   5  273   7616     0:00:02.234     0:15:57.460
notepad           26212   8   4  248   2872     0:00:00.234     0:15:43.529
MusNotifyIcon     19336   6   5  321   4280     0:00:00.515     0:14:19.713
SnippingTool       8840   8  16  650  13840     0:00:04.453     0:11:58.477
```

Toan Ngo
Date:3/6/24



```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>procdump -nobanner -mm 26212
[10:03:59] Dump 1 initiated: C:\Users\Toan C Ngo\Desktop\New folder (3)\tool\notepad.exe_240306_100359.dmp
[10:04:00] Dump 1 complete: 1 MB written in 1.0 seconds
[10:04:00] Dump count reached.


C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>
```

(now we create a dump file for the notepad process that we have opened, and this is where the pid comes into play. I call the function procdump(process dump create a dump of a process) -nobanner -mm ((this is the dumping type, there like 4 dump type total and those are mm=mini dump ,ma=full dump ,mt=triage dump and mk=kernel dump)and in this case i create a mini dump) 26212 (this is the id of the process that we get from the previous pslist. After this has finished running it should create a mini dump of the process that was mapped to the id of 26212 in the current directory.)

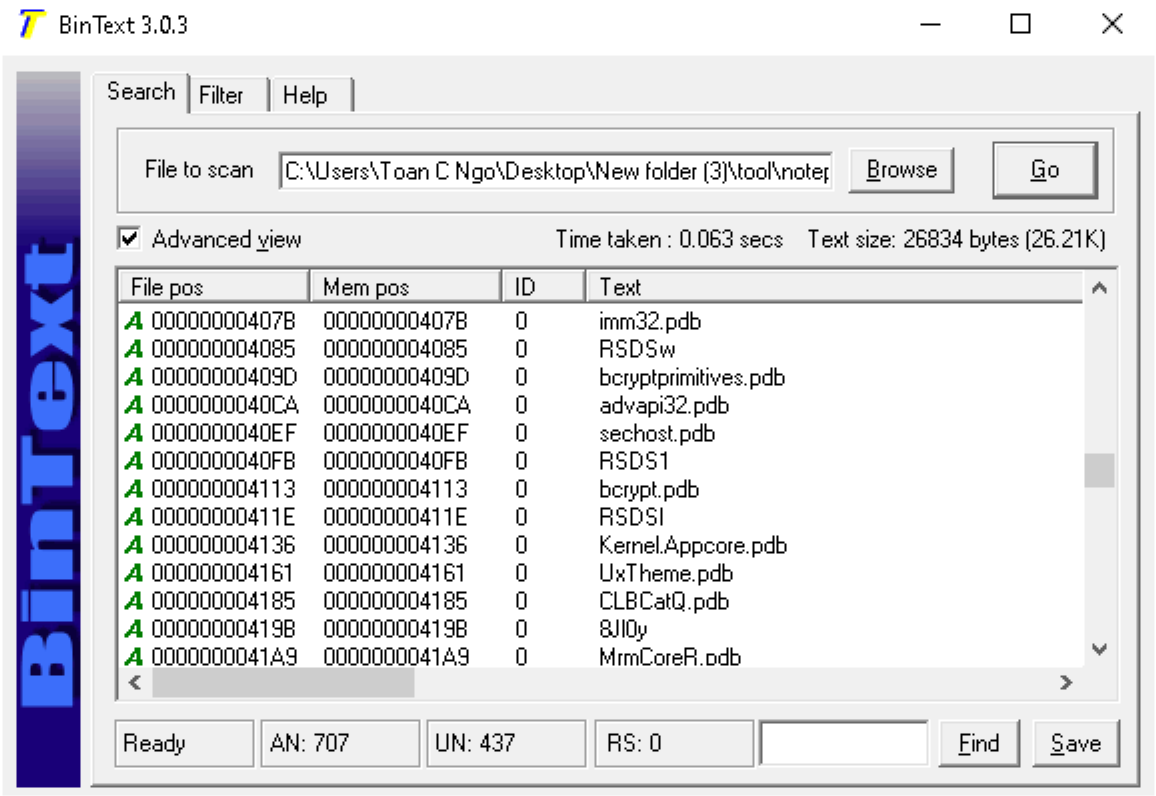


```
movefile64                      9/3/2020 11:07 AM     Application
notepad.exe_240227_200033.dmp   2/27/2024 8:00 PM     DMP File
notepad.exe_240306_100359.dmp   3/6/2024 10:04 AM     DMP File
notmyfault                      9/29/2022 9:26 PM     Application
notmyfault64                    9/29/2022 9:26 PM     Application
```

(the output of the dump notepad file. (i have two because i already did this before, but in your case it it should just be one file))

For the next thing we are gonna do, go to this site https://github.com/mfput/McAfee-Tools and download the bintext303.
After you have downloaded the tool, extract them and open it up, you should see something like this, but without the file to scan part being filled.

Toan Ngo
Date:3/6/24



File to scan C:\Users\Toan C Ngo\Desktop\New folder (3)\tool\notep

☑ Advanced view

Time taken : 0.063 secs Text size: 26834 bytes (26.21K)

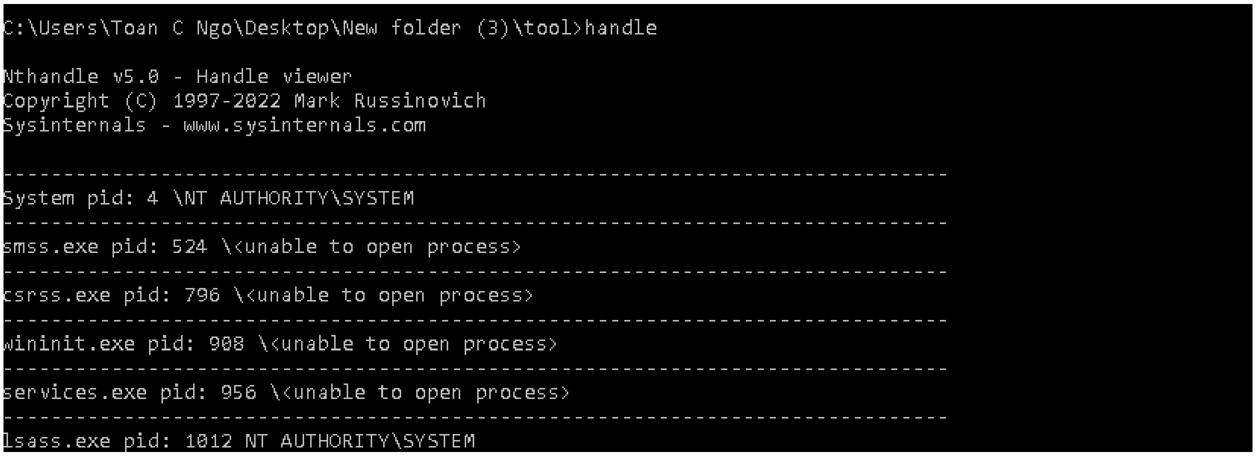
File pos	Mem pos	ID	Text
A 00000000407B	00000000407B	0	imm32.pdb
A 000000004085	000000004085	0	RSDSw
A 00000000409D	00000000409D	0	bcryptprimitives.pdb
A 0000000040CA	0000000040CA	0	advapi32.pdb
A 0000000040EF	0000000040EF	0	sechost.pdb
A 0000000040FB	0000000040FB	0	RSDS1
A 000000004113	000000004113	0	bcrypt.pdb
A 00000000411E	00000000411E	0	RSDSI
A 000000004136	000000004136	0	Kernel.Appcore.pdb
A 000000004161	000000004161	0	UxTheme.pdb
A 000000004185	000000004185	0	CLBCatQ.pdb
A 00000000419B	00000000419B	0	8JI0y
A 0000000041A9	0000000041A9	0	MrmCoreR.pdb

Ready AN: 707 UN: 437 RS: 0

(now that you have the tool you can click on the browse button and search for the dump file that you just have created and select it, afterward click the go button and it should just display you something like this. This tool helps you see what types of information are stored in the dump ie the content of the dumb file, so what you see here are what is being stored in the file.)

Next we are going to look into Handles. So when a process is created the operating system will then be giving a set of handles to that process and mapping them together,which these handles can be used from the internal function to access resources that were made for that process. Handles could also work like a pointer where it finds and locate the correct file in some programming languages.

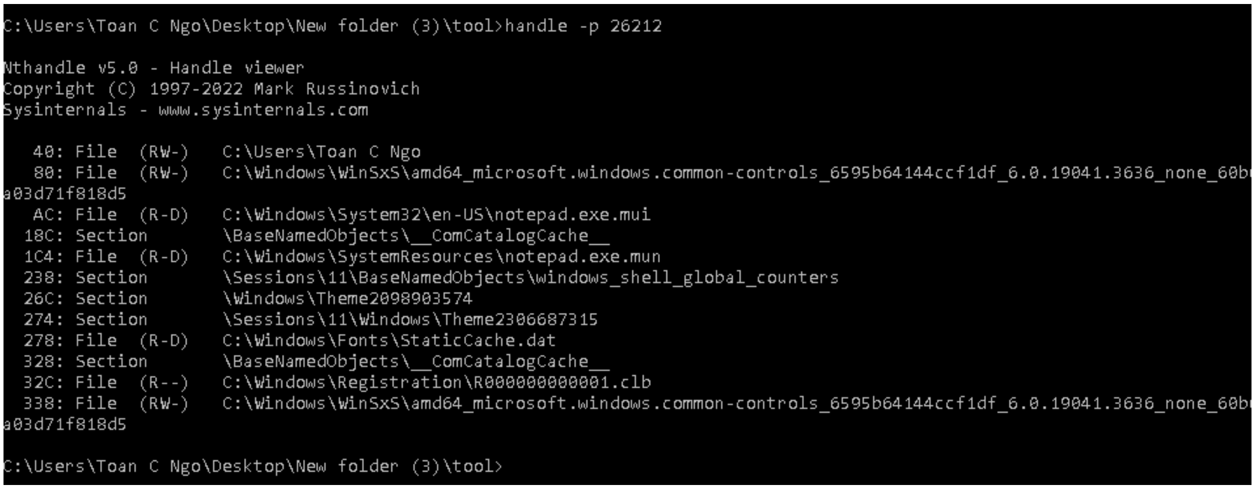
Toan Ngo
Date:3/6/24



```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>handle

Nthandle v5.0 - Handle viewer
Copyright (C) 1997-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

------------------------------------------------------------------------------
System pid: 4 \NT AUTHORITY\SYSTEM
------------------------------------------------------------------------------
smss.exe pid: 524 \<unable to open process>
------------------------------------------------------------------------------
csrss.exe pid: 796 \<unable to open process>
------------------------------------------------------------------------------
wininit.exe pid: 908 \<unable to open process>
------------------------------------------------------------------------------
services.exe pid: 956 \<unable to open process>
------------------------------------------------------------------------------
lsass.exe pid: 1012 NT AUTHORITY\SYSTEM
```

(this will display all the handles in your current active system (i recommend you don't do this if you don't need to see add process handle))

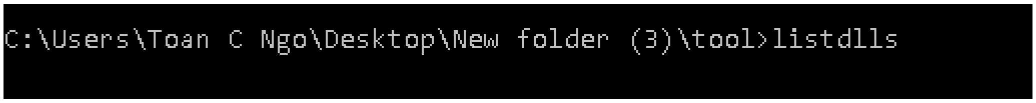
Instead do this



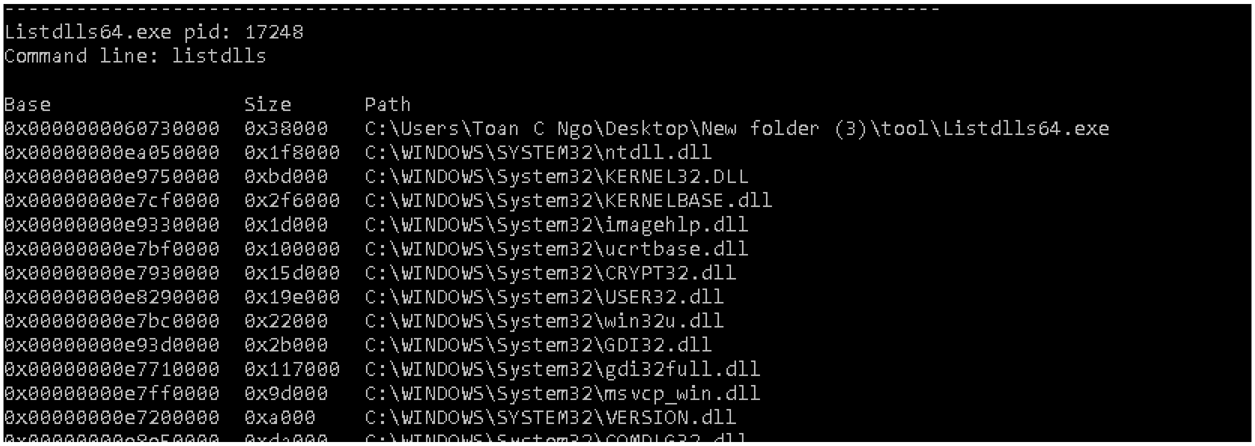
```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>handle -p 26212

Nthandle v5.0 - Handle viewer
Copyright (C) 1997-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

   40: File  (RW-)   C:\Users\Toan C Ngo
   80: File  (RW-)   C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.3636_none_60b
a03d71f818d5
   AC: File  (R-D)   C:\Windows\System32\en-US\notepad.exe.mui
  18C: Section       \BaseNamedObjects\__ComCatalogCache__
  1C4: File  (R-D)   C:\Windows\SystemResources\notepad.exe.mun
  238: Section       \Sessions\11\BaseNamedObjects\windows_shell_global_counters
  26C: Section       \Windows\Theme2098903574
  274: Section       \Sessions\11\Windows\Theme2306687315
  278: File  (R-D)   C:\Windows\Fonts\StaticCache.dat
  328: Section       \BaseNamedObjects\__ComCatalogCache__
  32C: File  (R--)   C:\Windows\Registration\R000000000001.clb
  338: File  (RW-)   C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.3636_none_60b
a03d71f818d5

C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>
```

(so what i did here is that i call handle but with a condition of getting only the relevance process by id(pid).
code: Handle(function) -p(process) 26212(id).)

Same thing can be said for Dlls(dynamic links library).



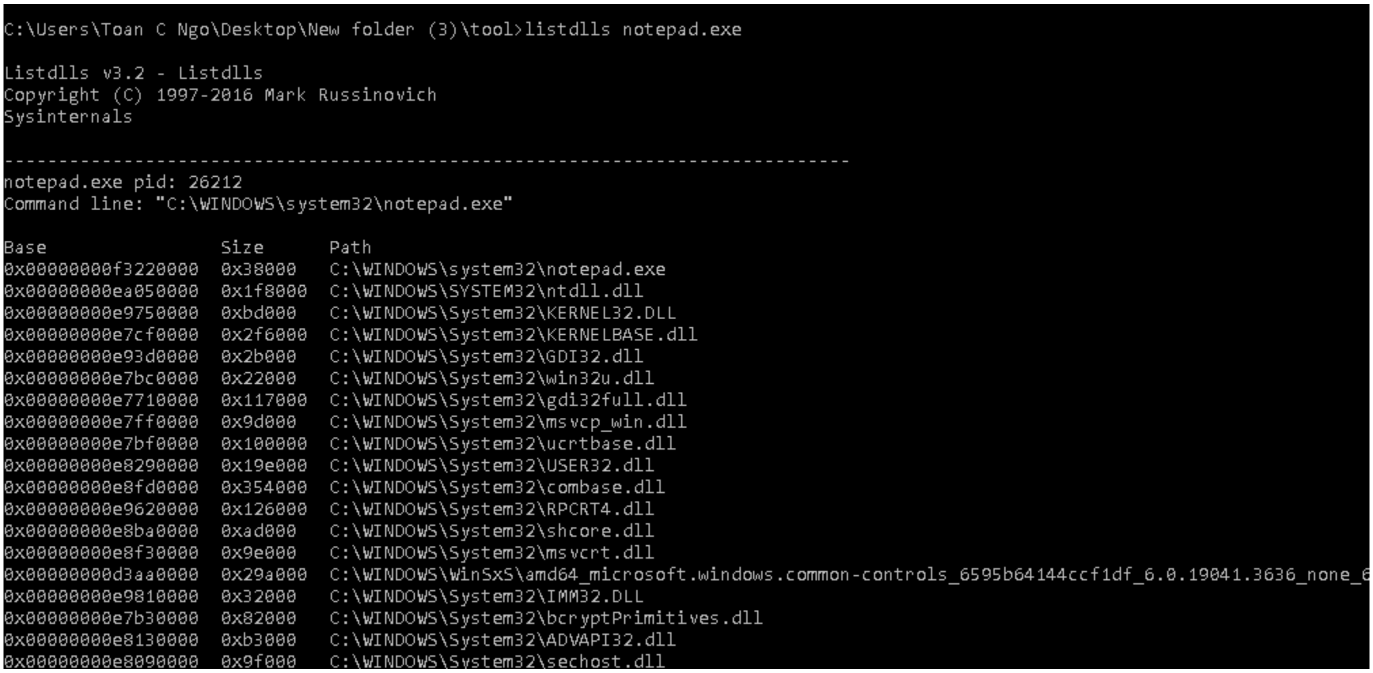
```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>listdlls
```



```
------------------------------------------------------------------------------
Listdlls64.exe pid: 17248
Command line: listdlls

Base                  Size      Path
0x0000000060730000  0x38000   C:\Users\Toan C Ngo\Desktop\New folder (3)\tool\Listdlls64.exe
0x00000000ea050000  0x1f8000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000e9750000  0xbd000   C:\WINDOWS\System32\KERNEL32.DLL
0x00000000e7cf0000  0x2f6000  C:\WINDOWS\System32\KERNELBASE.dll
0x00000000e9330000  0x1d000   C:\WINDOWS\System32\imagehlp.dll
0x00000000e7bf0000  0x100000  C:\WINDOWS\System32\ucrtbase.dll
0x00000000e7930000  0x15d000  C:\WINDOWS\System32\CRYPT32.dll
0x00000000e8290000  0x19e000  C:\WINDOWS\System32\USER32.dll
0x00000000e7bc0000  0x22000   C:\WINDOWS\System32\win32u.dll
0x00000000e93d0000  0x2b000   C:\WINDOWS\System32\GDI32.dll
0x00000000e7710000  0x117000  C:\WINDOWS\System32\gdi32full.dll
0x00000000e7ff0000  0x9d000   C:\WINDOWS\System32\msvcp_win.dll
0x00000000e7200000  0xa000    C:\WINDOWS\SYSTEM32\VERSION.dll
0x00000000e8e50000  0xda000   C:\WINDOWS\System32\COMDLG32.dll
```

(as you can see the output is is too big for me to screenshot it so recommend you don't do this if you only need to access one press Dlls information)

Instead do this



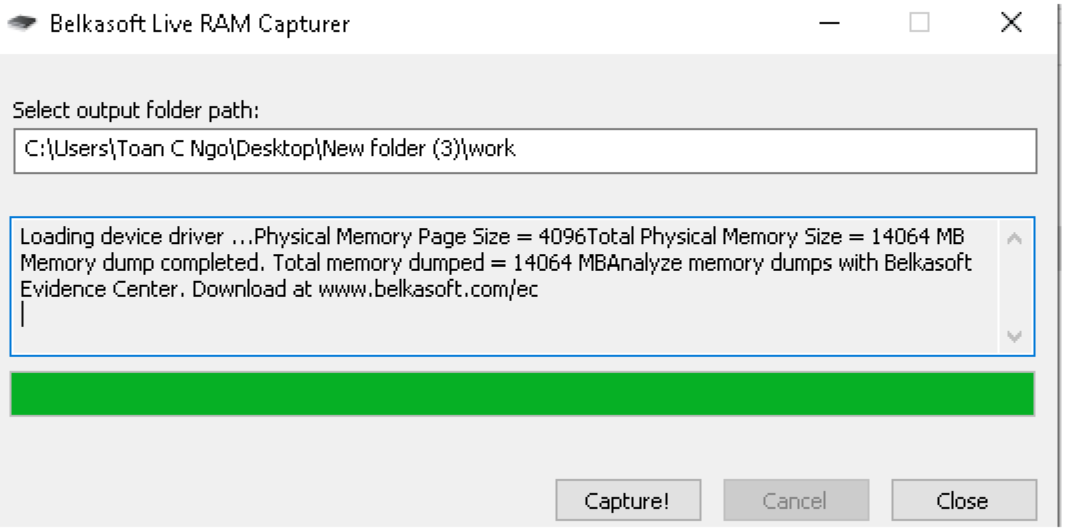
```
C:\Users\Toan C Ngo\Desktop\New folder (3)\tool>listdlls notepad.exe

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

------------------------------------------------------------------------------
notepad.exe pid: 26212
Command line: "C:\WINDOWS\system32\notepad.exe"

Base                Size      Path
0x00000000f3220000  0x38000   C:\WINDOWS\system32\notepad.exe
0x00000000ea050000  0x1f8000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000e9750000  0xbd000   C:\WINDOWS\System32\KERNEL32.DLL
0x00000000e7cf0000  0x2f6000  C:\WINDOWS\System32\KERNELBASE.dll
0x00000000e93d0000  0x2b000   C:\WINDOWS\System32\GDI32.dll
0x00000000e7bc0000  0x22000   C:\WINDOWS\System32\win32u.dll
0x00000000e7710000  0x117000  C:\WINDOWS\System32\gdi32full.dll
0x00000000e7ff0000  0x9d000   C:\WINDOWS\System32\msvcp_win.dll
0x00000000e7bf0000  0x100000  C:\WINDOWS\System32\ucrtbase.dll
0x00000000e8290000  0x19e000  C:\WINDOWS\System32\USER32.dll
0x00000000e8fd0000  0x354000  C:\WINDOWS\System32\combase.dll
0x00000000e9620000  0x126000  C:\WINDOWS\System32\RPCRT4.dll
0x00000000e8ba0000  0xad000   C:\WINDOWS\System32\shcore.dll
0x00000000e8f30000  0x9e000   C:\WINDOWS\System32\msvcrt.dll
0x00000000d3aa0000  0x29a000  C:\WINDOWS\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.3636_none_6
0x00000000e9810000  0x32000   C:\WINDOWS\System32\IMM32.DLL
0x00000000e7b30000  0x82000   C:\WINDOWS\System32\bcryptPrimitives.dll
0x00000000e8130000  0xb3000   C:\WINDOWS\System32\ADVAPI32.dll
0x00000000e8090000  0x9f000   C:\WINDOWS\System32\sechost.dll
```

(this will only give you all the relative information about the dlls of the select application only, and in may case i can only get the dlls for the application of notepad.exe only and nothing else.)

And finally the ram acquisition
First you will need this tool Belkasoft ram capture and you can get this tool from here(https://belkasoft.com/ram-capturer) you do need to give them your email and they will respond back with the download link for the software, but from my experience i think any email will do just fine. What this tool does is that it will

Toan Ngo
Date:3/6/24

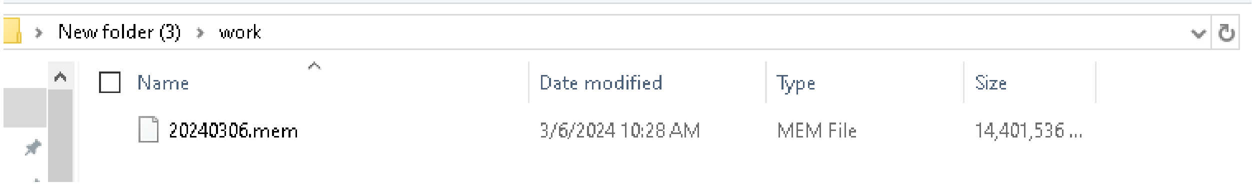
capture the current ram that is running in your pc and output it as a .mem extension for analysts but for now we just need to capture the ram.



Select output folder path:
C:\Users\Toan C Ngo\Desktop\New folder (3)\work

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 14064 MB
Memory dump completed. Total memory dumped = 14064 MBAnalyze memory dumps with Belkasoft
Evidence Center. Download at www.belkasoft.com/ec
```

(Here i capture the ram and stored the output in the difference directory name work)



Name	Date modified	Type	Size
20240306.mem	3/6/2024 10:28 AM	MEM File	14,401,536 ...

(And here is the output after the software is done running. You can now take the .mem file to analyze if you wanted to)

In conclusion the dump files serve an extremely importance function, and that is to keep a report on your operating system if something were to happen to it, and it also responsible for outputting the file that contain a report on what happened to the machine for the user to analyze and fix at a later date.

Toan Ngo
Date:3/6/24

Resources

Crash dump info:
https://techcommunity.microsoft.com/t5/ask-the-performance-team/understanding-crash-dump-files/ba-p/372633

What is the purpose of a dump file:
https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/memory-dump-file-options

Type of dump:
https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/varieties-of-kernel-mode-dump-files

Usefulness of dump:
https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/analyzing-a-user-mode-dump-file

Most information are from Lap7 resource from cs-362

Application resource :
Belkasoft ram capture: https://belkasoft.com/ram-capturer
Bintext303: https://github.com/mfput/McAfee-Tools