LAB 9

Name: ARAVINDHAN.K

ROLL NO:CH.EN.U4CYS22001

Introduction to Memory Forensics

Memory forensics is a crucial aspect of cyber investigations, allowing forensic analysts to extract valuable artifacts from volatile memory (RAM). This lab focuses on using **DumpIt** for capturing memory dumps and **Volatility 3** for in-depth analysis. Additionally, we explore **Redline**, a GUI-based forensic analysis tool.

Section 1: DumpIt - Easiest Tool for Capturing RAM

Overview:

DumpIt is a lightweight tool designed for quickly acquiring memory dumps from a system. It is highly effective in forensic investigations and requires minimal setup.

Steps to Capture RAM using DumpIt:

1. **Download and Run DumpIt**

   ○ Download **DumpIt.exe** and place it on the target system. ○ Right-click and **Run as Administrator**.

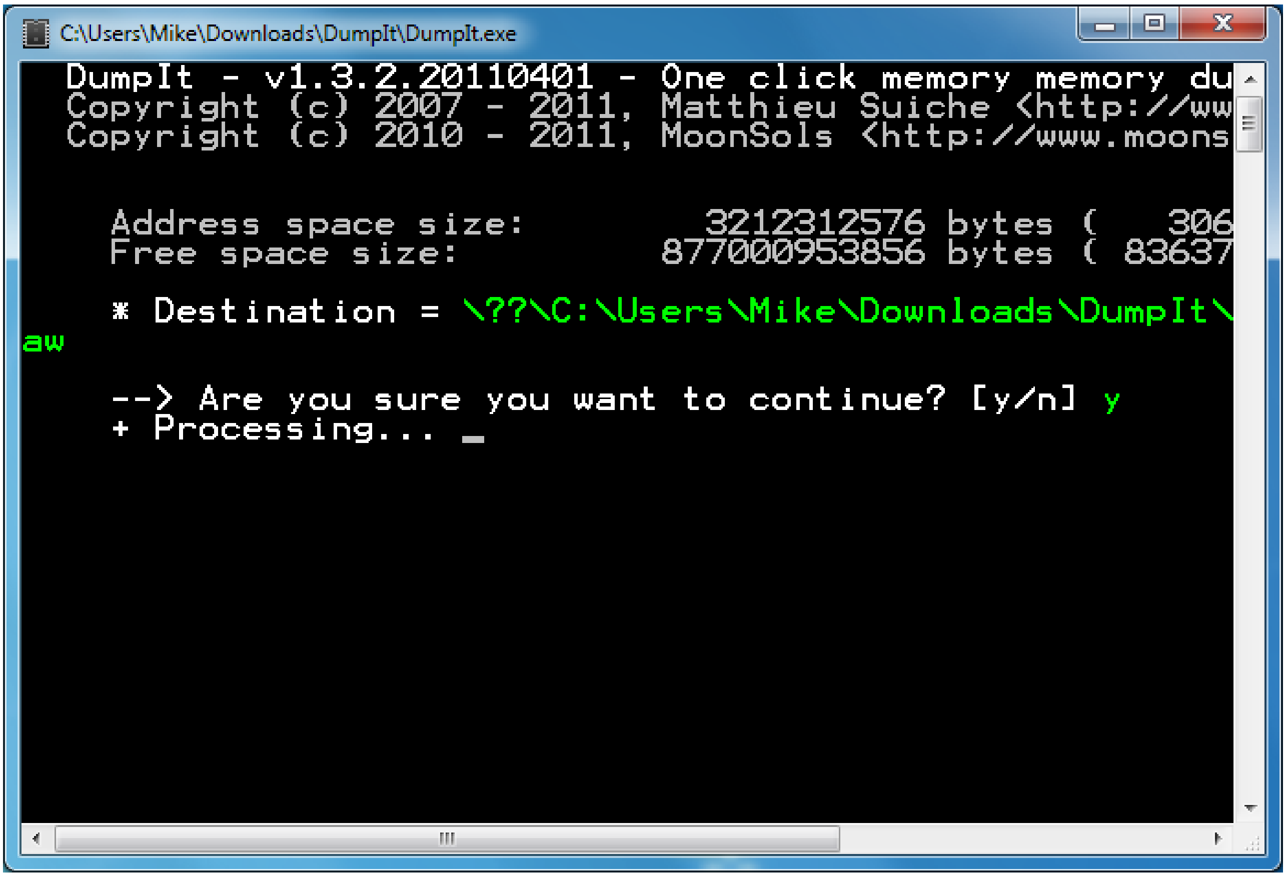
2. **Memory Dump Generation**

   ○ Once executed, DumpIt creates a **.raw** memory dump file in the same directory. ○ The output file will be named something like `memory.raw`.

3. **Prepare for Analysis**

   ○ Transfer the `.raw` file to a forensic workstation for analysis using **Volatility 3**.

Screenshot Placeholder:



```
  DumpIt - v1.3.2.20110401 - One click memory memory du
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://ww
  Copyright (c) 2010 - 2011, MoonSols <http://www.moons

    Address space size:        3212312576 bytes (   306
    Free space size:          877000953856 bytes ( 83637

    * Destination = \??\C:\Users\Mike\Downloads\DumpIt\
aw

    --> Are you sure you want to continue? [y/n] y
    + Processing... _
```

Section 2: Volatility 3 - Best for Memory Analysis

Overview:

Volatility 3 is an advanced memory forensics framework used for analyzing captured memory dumps. It can help detect malware, rootkits, processes, network connections, and more.

Installing Volatility 3

1. Open a terminal and clone the Volatility 3 repository:

```
git clone https://github.com/volatilityfoundation/volatility3.git
cd volatility3
```

2. Run the following command to check available options:

```
python3 vol.py -h
```

Running an Analysis (Process List Example)

Once the memory dump is captured, analyze it using Volatility 3:

```
python3 vol.py -f memory.raw windows.pslist
```

This command lists all active processes running at the time of the memory dump.

Additional Analysis Commands:

- Detect network connections:

```
python3 vol.py -f memory.raw windows.netscan
```

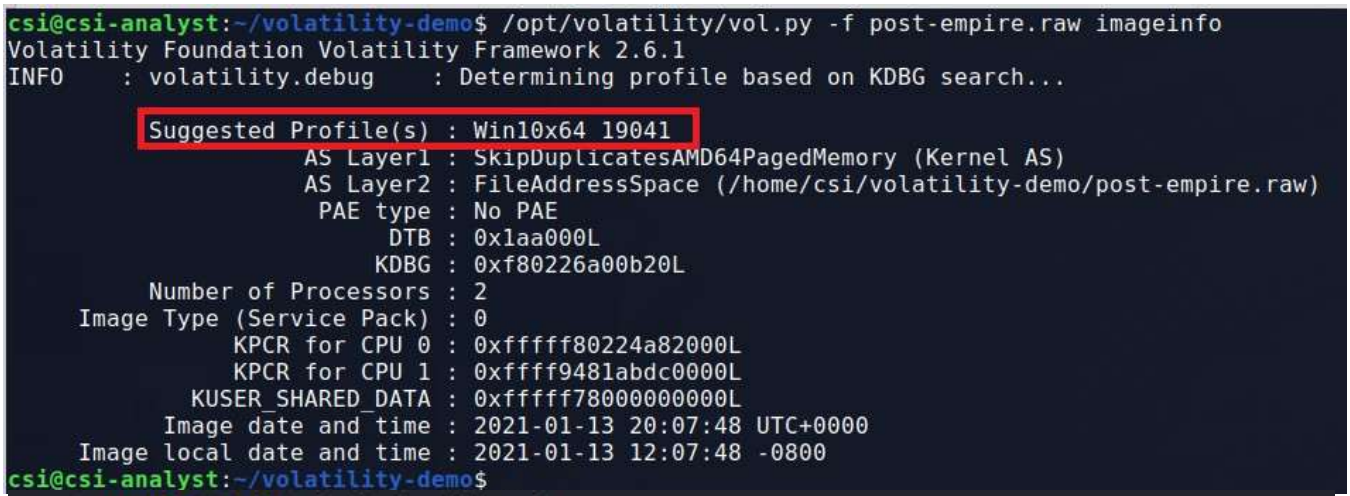
- Check loaded DLLs:

```
python3 vol.py -f memory.raw windows.dlllist
```

- Analyze registry hives:

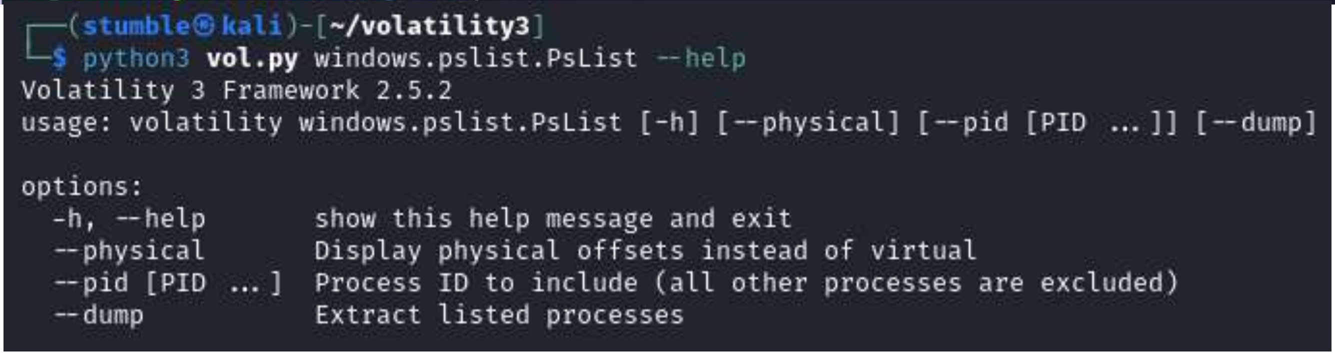
```
python3 vol.py -f memory.raw windows.registry.hivelist
```

Screenshot Placeholder:



```
csi@csi-analyst:~/volatility-demo$ /opt/volatility/vol.py -f post-empire.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...

          Suggested Profile(s) : Win10x64_19041
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/csi/volatility-demo/post-empire.raw)
                      PAE type : No PAE
                           DTB : 0x1aa000L
                          KDBG : 0xf80226a00b20L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80224a82000L
                KPCR for CPU 1 : 0xffff9481abdc0000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2021-01-13 20:07:48 UTC+0000
     Image local date and time : 2021-01-13 12:07:48 -0800
csi@csi-analyst:~/volatility-demo$
```



```
┌──(stumble㉿kali)-[~/volatility3]
└─$ python3 vol.py windows.pslist.PsList --help
Volatility 3 Framework 2.5.2
usage: volatility windows.pslist.PsList [-h] [--physical] [--pid [PID ...]] [--dump]

options:
  -h, --help         show this help message and exit
  --physical         Display physical offsets instead of virtual
  --pid [PID ...]    Process ID to include (all other processes are excluded)
  --dump             Extract listed processes
```

Section 3: Redline - Best GUI-Based Memory Analysis

Overview:

FireEye **Redline** provides a user-friendly interface for analyzing forensic artifacts, especially useful for those preferring a graphical approach.

Steps to Use Redline:

1. **Download and Install**

    ○ Download **FireEye Redline** from the official website. ○ Install and launch the tool.

2. **Collecting Memory Data**

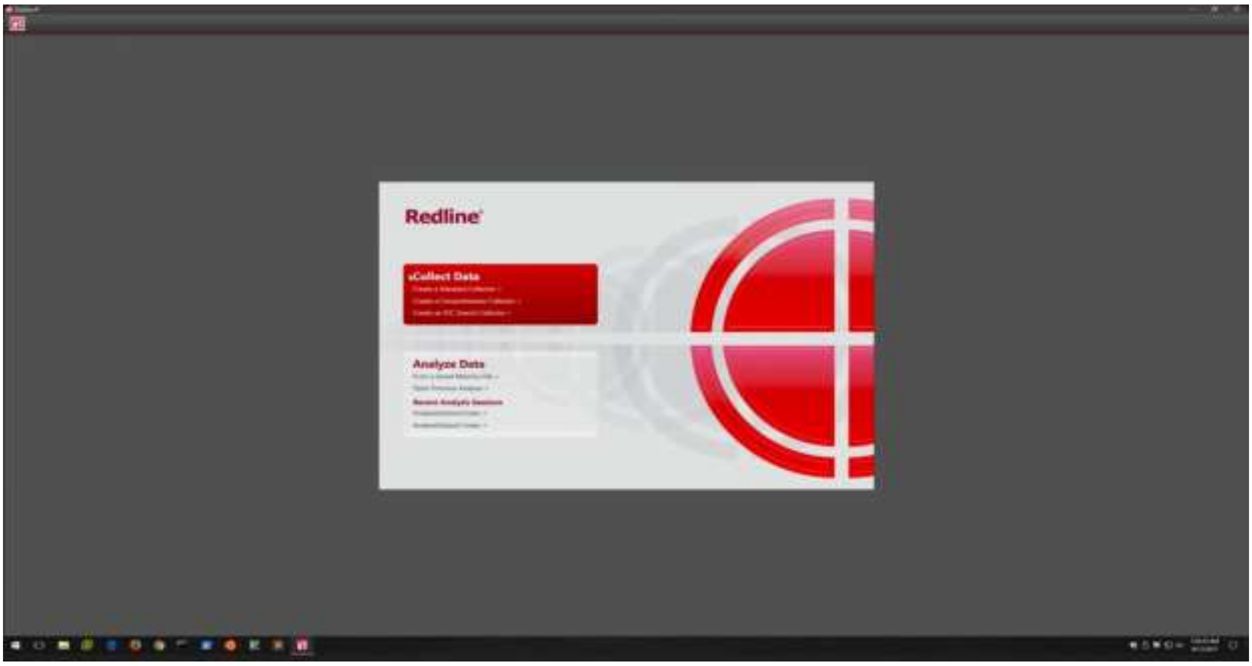
    ○ Open Redline and navigate to **"Collect Data"**.

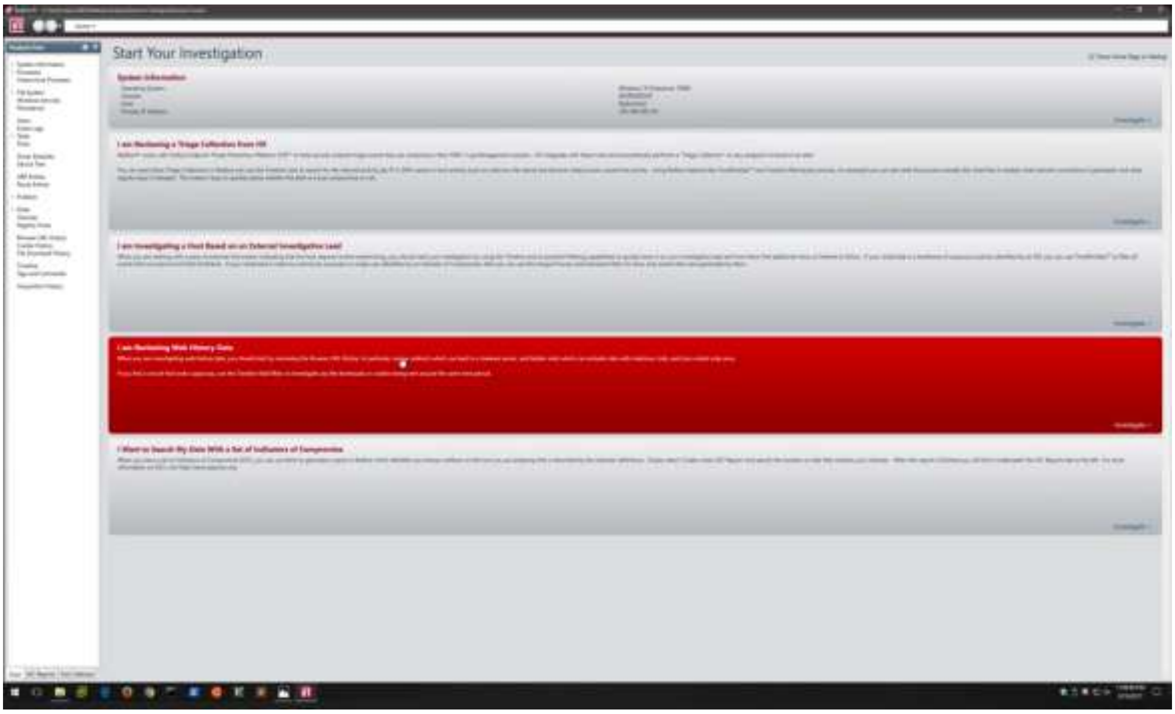
    ○ Choose the target system and initiate the scan.

3. **Analyzing Results**

    ○ Redline provides visualizations such as graphs, timelines, and alerts for suspicious activity detection.

Screenshot Placeholder:

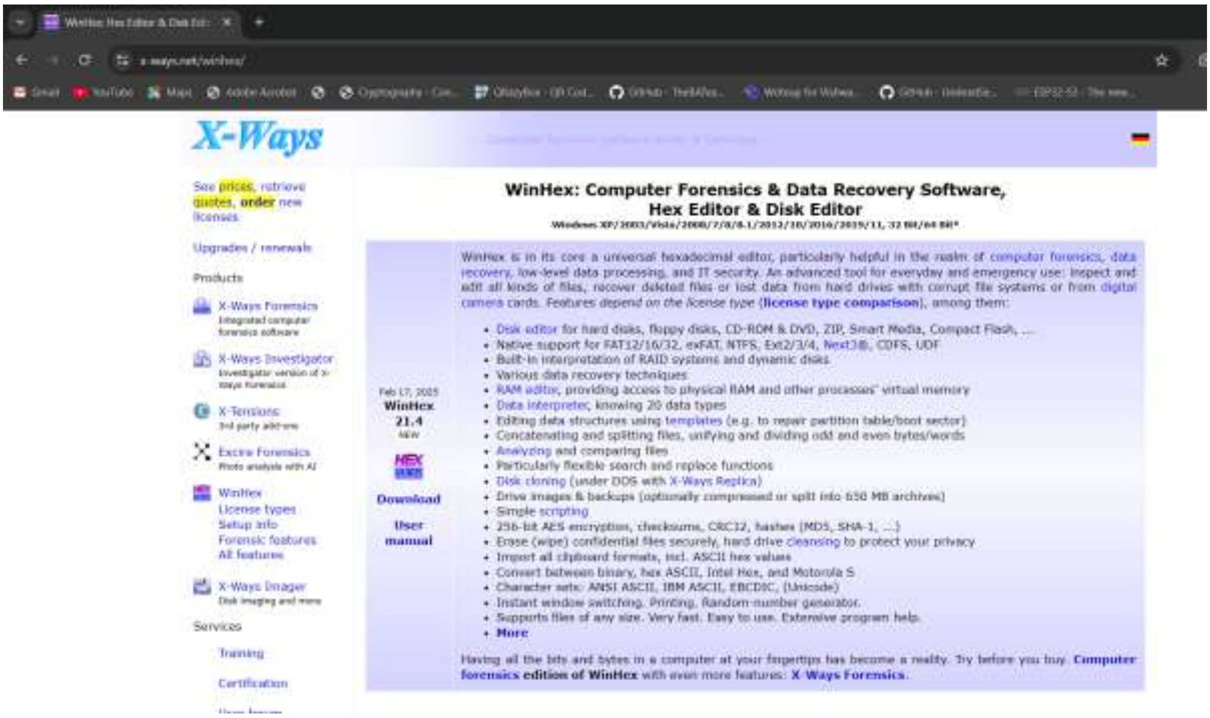




Start Your Investigation
System Information
I am Reviewing a Triage Collection from HX
I am Investigating a Host Based on an External Investigation Lead
I am Reviewing Web History Data
I Want to Search My Data With a Set of Indicators of Compromise

SLACK AND SWAP SPACE

Install winhex



WinHex: Computer Forensics & Data Recovery Software,
Hex Editor & Disk Editor
Windows XP/2003/Vista/2008/7/8/8.1/2012/10/2016/2019/11, 32 Bit/64 Bit*

WinHex is in its core a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security. An advanced tool for everyday and emergency use: inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards. Features depend *on the license* type (**license type comparison**), among them:

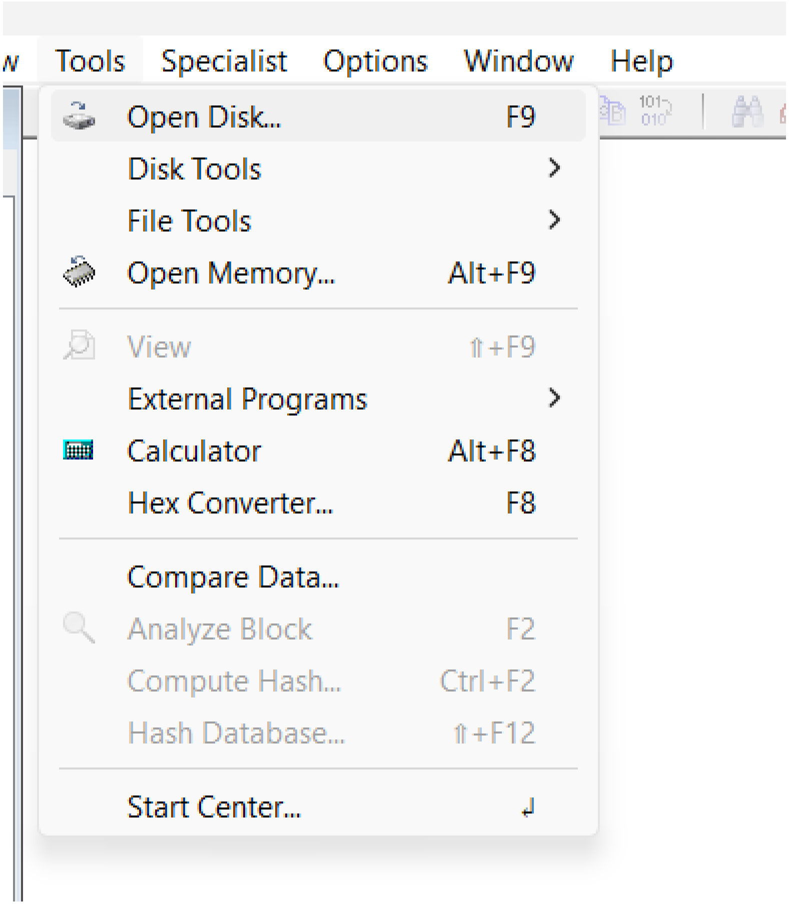
- Disk editor for hard disks, floppy disks, CD-ROM & DVD, ZIP, Smart Media, Compact Flash, ...
- Native support for FAT12/16/32, exFAT, NTFS, Ext2/3/4, Next3®, CDFS, UDF
- Built-in interpretation of RAID systems and dynamic disks
- Various data recovery techniques
- RAM editor, providing access to physical RAM and other processes' virtual memory
- Data interpreter, knowing 20 data types
- Editing data structures using templates (e.g. to repair partition table/boot sector)
- Concatenating and splitting files, unifying and dividing odd and even bytes/words
- Analyzing and comparing files
- Particularly flexible search and replace functions
- Disk cloning (under DOS with X-Ways Replica)
- Drive images & backups (optionally compressed or split into 650 MB archives)
- Simple scripting
- 256-bit AES encryption, checksums, CRC32, hashes (MD5, SHA-1, ...)
- Erase (wipe) confidential files securely, hard drive cleansing to protect your privacy
- Import all clipboard formats, incl. ASCII hex values
- Convert between binary, hex ASCII, Intel Hex, and Motorola S
- Character sets: ANSI ASCII, IBM ASCII, EBCDIC, (Unicode)
- Instant window switching. Printing. Random-number generator.
- Supports files of any size. Very fast. Easy to use. Extensive program help.
- **More**

Having all the bits and bytes in a computer at your fingertips has become a reality. Try before you buy. **Computer forensics edition of WinHex** with even more features: **X-Ways Forensics**.

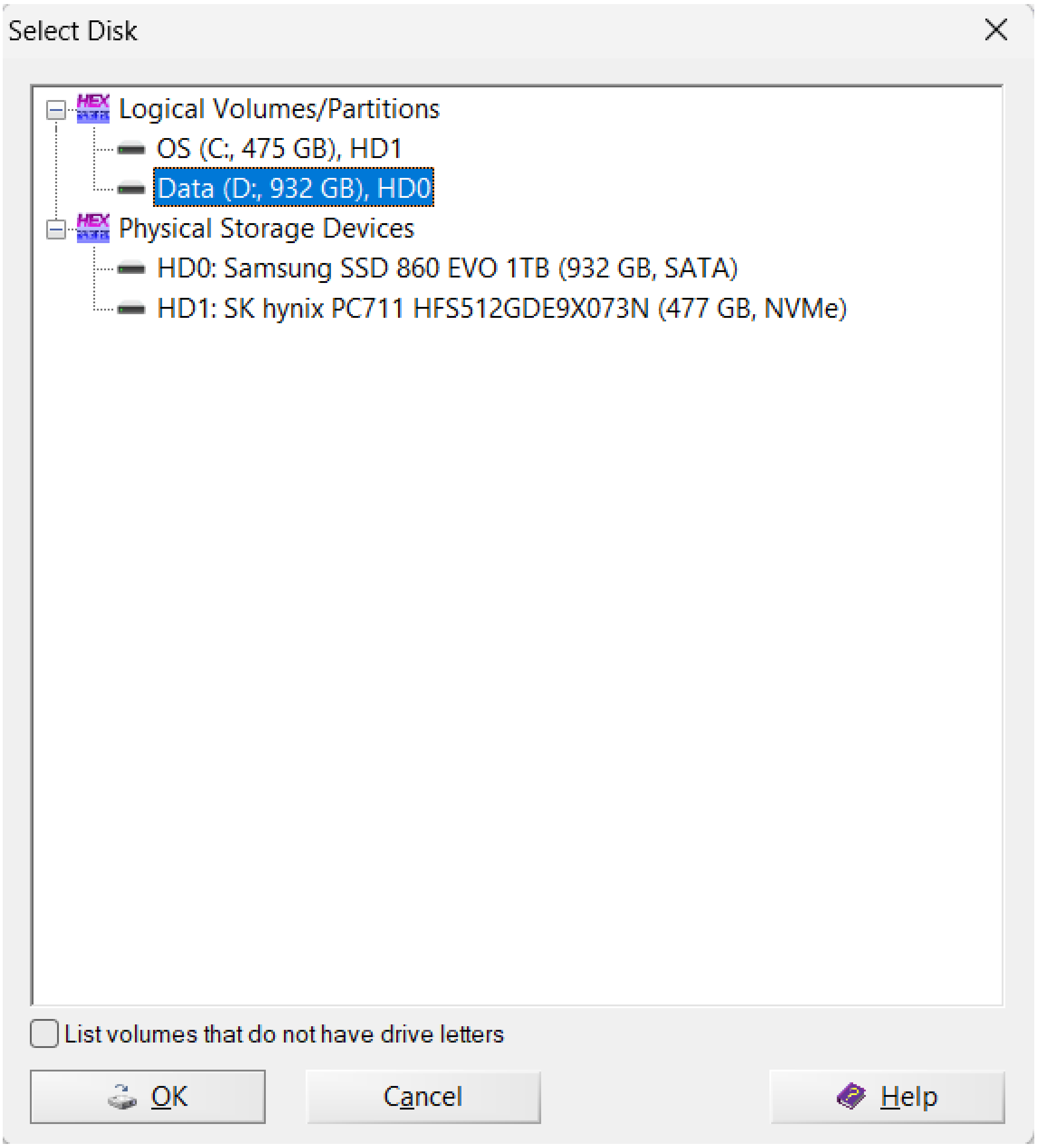
From the above website

And the winhex.exe in administrator mode right click and run has administrator

Go to Tools and click a open disk or F9



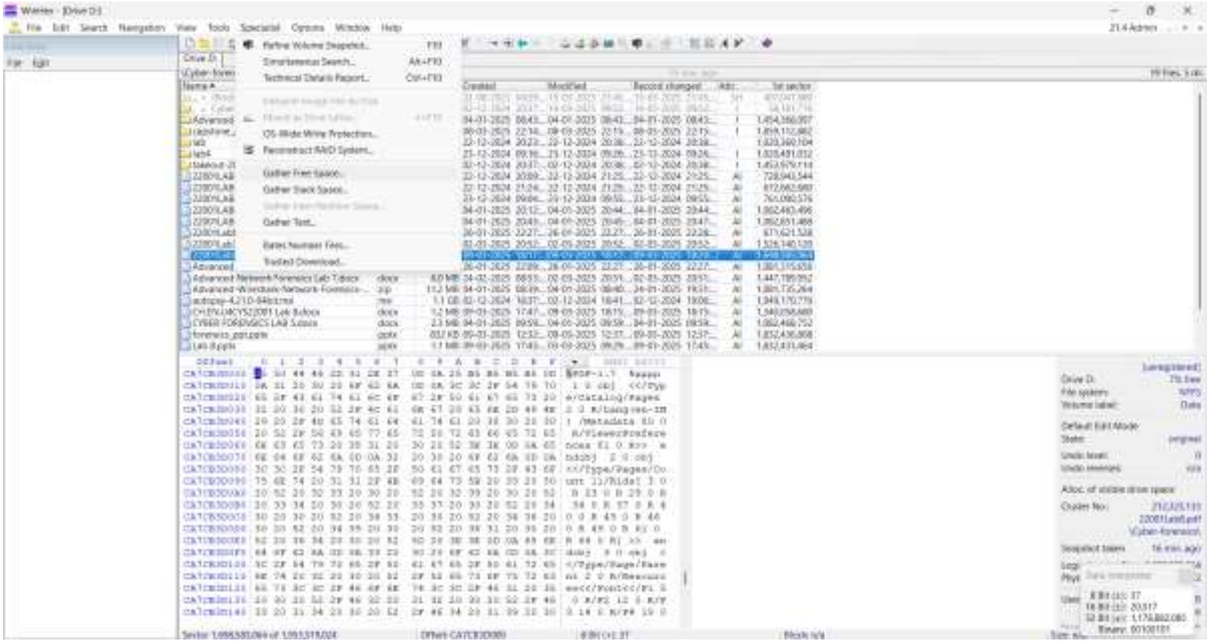
Choose a disk



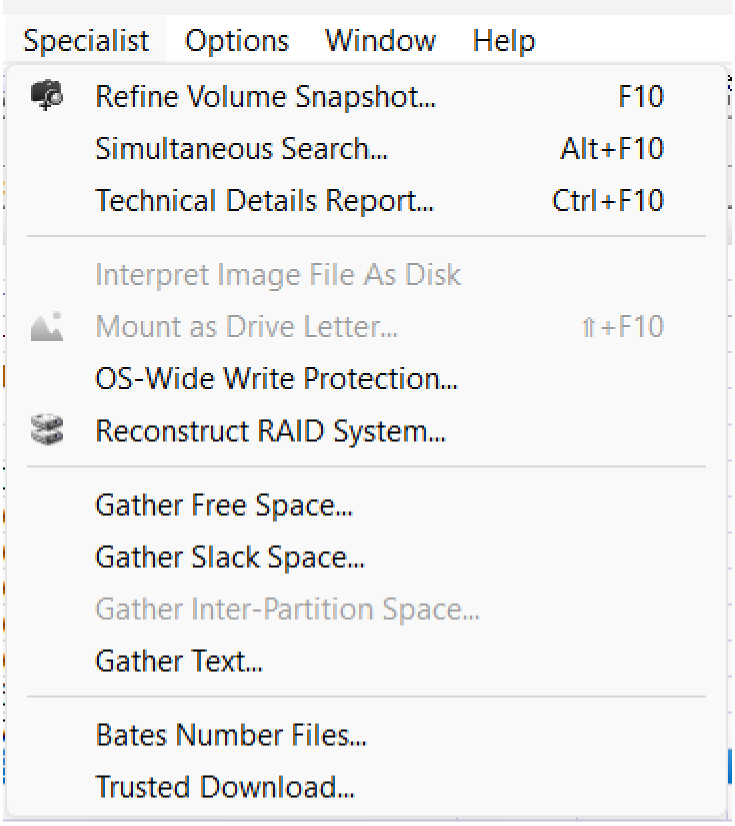
Select Disk

- Logical Volumes/Partitions
  - OS (C:, 475 GB), HD1
  - Data (D:, 932 GB), HD0
- Physical Storage Devices
  - HD0: Samsung SSD 860 EVO 1TB (932 GB, SATA)
  - HD1: SK hynix PC711 HFS512GDE9X073N (477 GB, NVMe)

□ List volumes that do not have drive letters

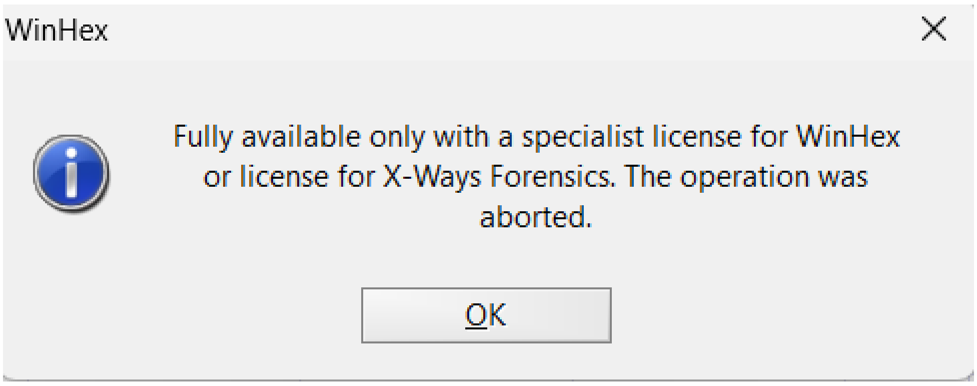


Next go to specialist option


Specialist
Options
Window
Help
Refine Volume Snapshot... F10
Simultaneous Search... Alt+F10
Technical Details Report... Ctrl+F10
Interpret Image File As Disk
Mount as Drive Letter... ⇧+F10
OS-Wide Write Protection...
Reconstruct RAID System...
Gather Free Space...
Gather Slack Space...
Gather Inter-Partition Space...
Gather Text...
Bates Number Files...
Trusted Download...

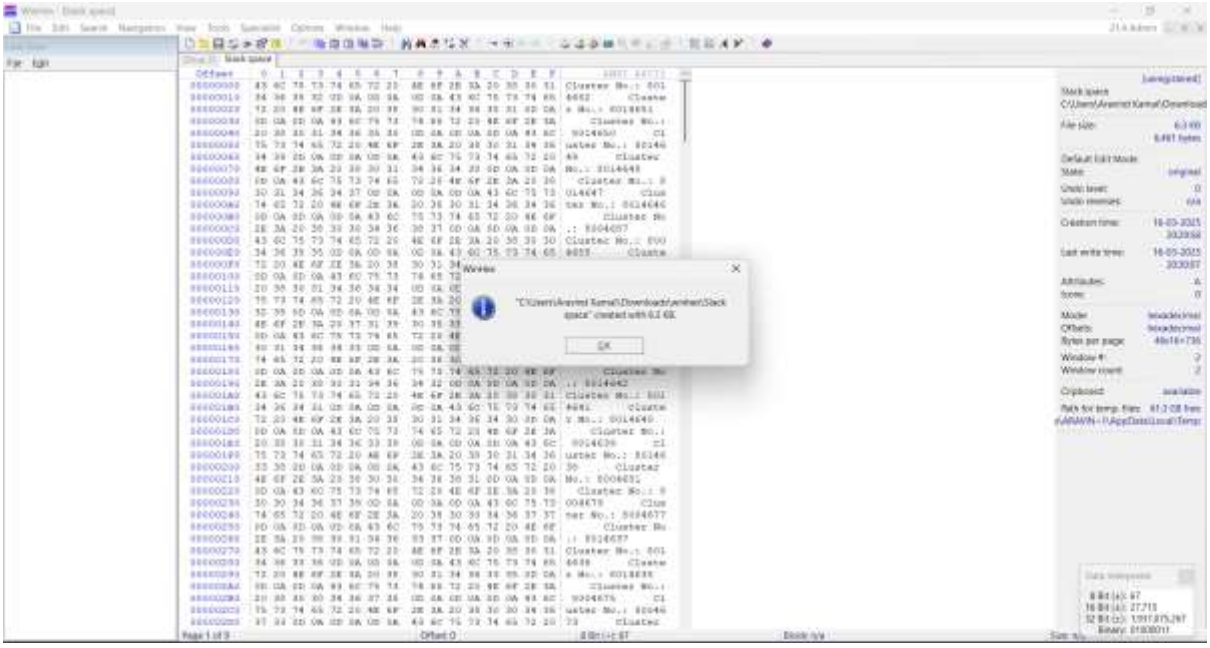
And click gather slack space

Due to software version it has some limited options in normal version in paid it has more options



WinHex

Fully available only with a specialist license for WinHex or license for X-Ways Forensics. The operation was aborted.

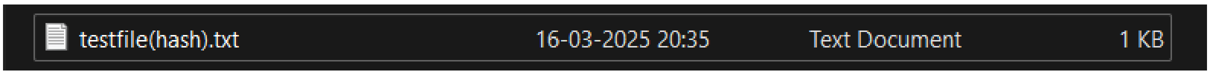


"C:\Users\Aravind Kamal\Downloads\winhex\Slack space" created with 6.2 KB.

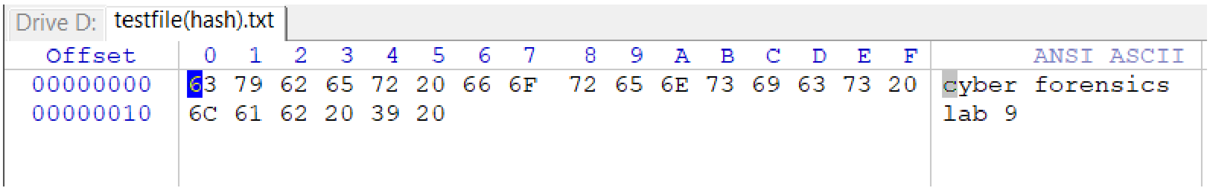
Slack space is viewed

Compute Hash

- Try various Hash functions for a particular file or folder



testfile(hash).txt 16-03-2025 20:35 Text Document 1 KB

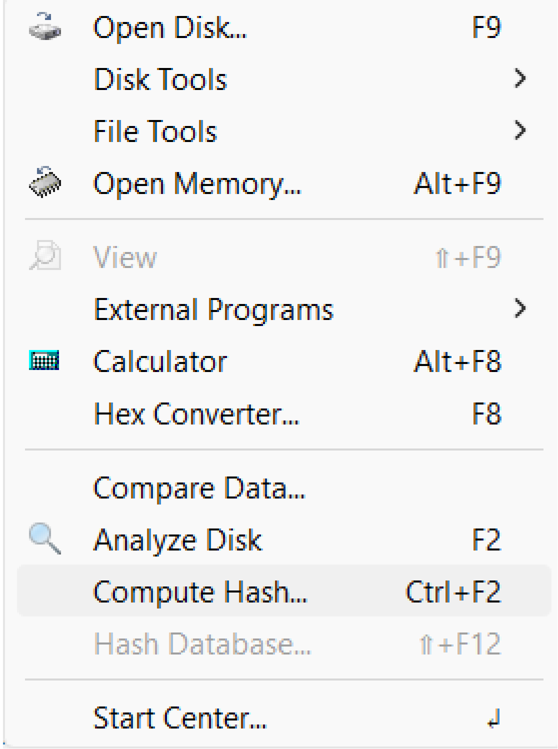


```
Drive D: testfile(hash).txt
  Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
 00000000    63 79 62 65 72 20 66 6F  72 65 6E 73 69 63 73 20   cyber forensics
 00000010    6C 61 62 20 39 20                                  lab 9
```

Let us take this file

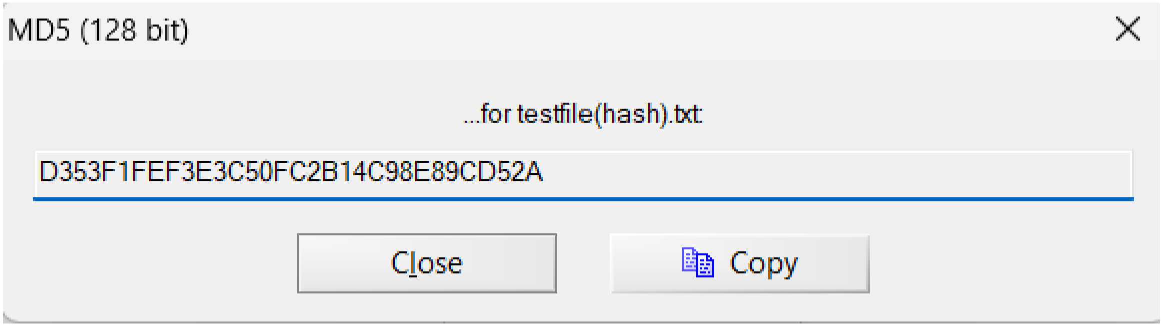
And find the hash go to winhex

And find the hash



Under tools

For MD5

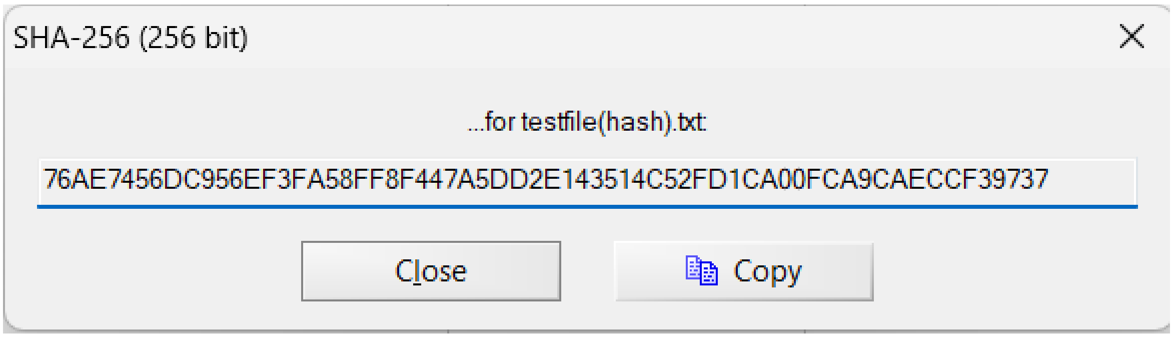


...for testfile(hash).txt:

D353F1FEF3E3C50FC2B14C98E89CD52A

Try some other hashes too

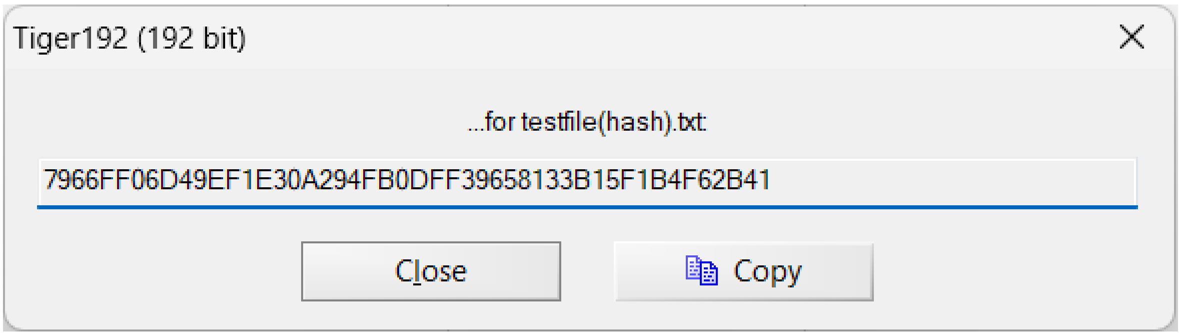
SHA -256



...for testfile(hash).txt:

76AE7456DC956EF3FA58FF8F447A5DD2E143514C52FD1CA00FCA9CAECCF39737

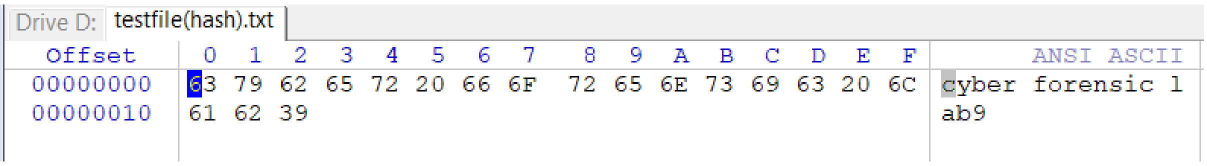
Tiger 192 hash



...for testfile(hash).txt:

7966FF06D49EF1E30A294FB0DFF39658133B15F1B4F62B41

Now we can alter the file some text



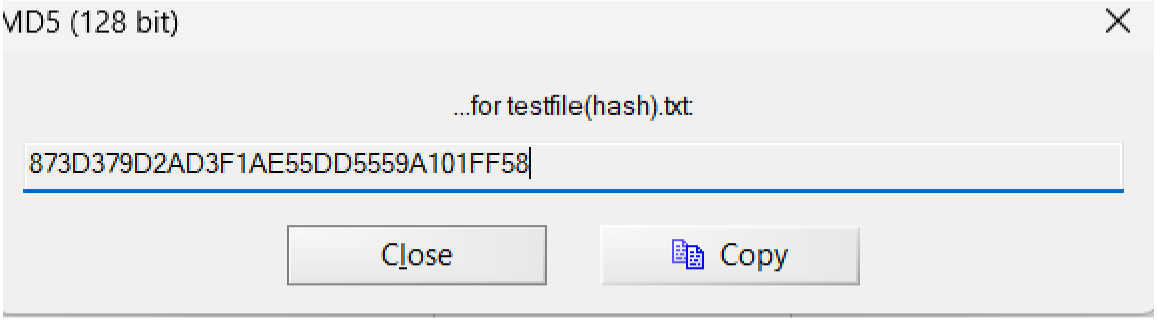
```
 Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F      ANSI ASCII
00000000    63 79 62 65 72 20 66 6F  72 65 6E 73 69 63 20 6C   cyber forensic l
00000010    61 62 39                                           ab9
```

And again checking hash of the file

- Recheck the hash and prove that there has been an modification

Checking

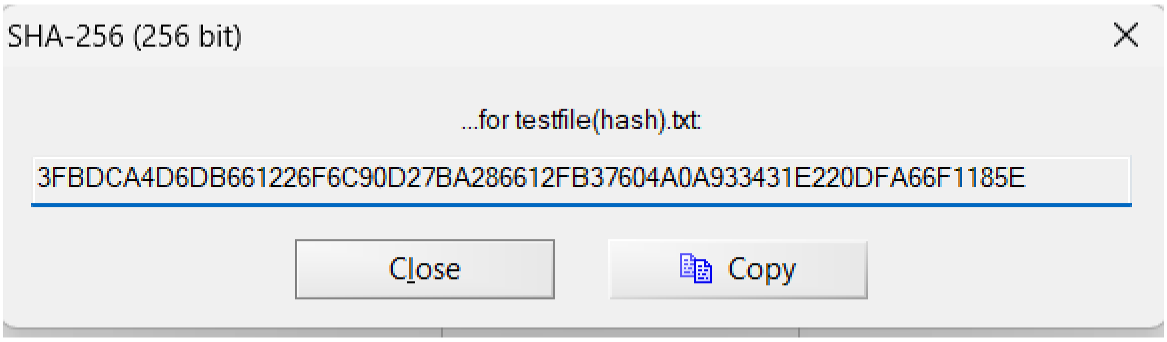
MD5



873D379D2AD3F1AE55DD5559A101FF58

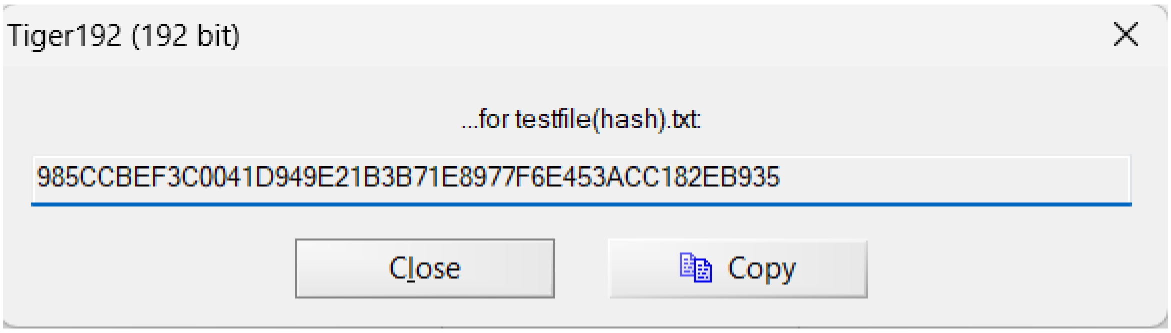
See we can see the value changed

Now for sha-256



3FBDCA4D6DB661226F6C90D27BA286612FB37604A0A933431E220DFA66F1185E

Now Tiger 192



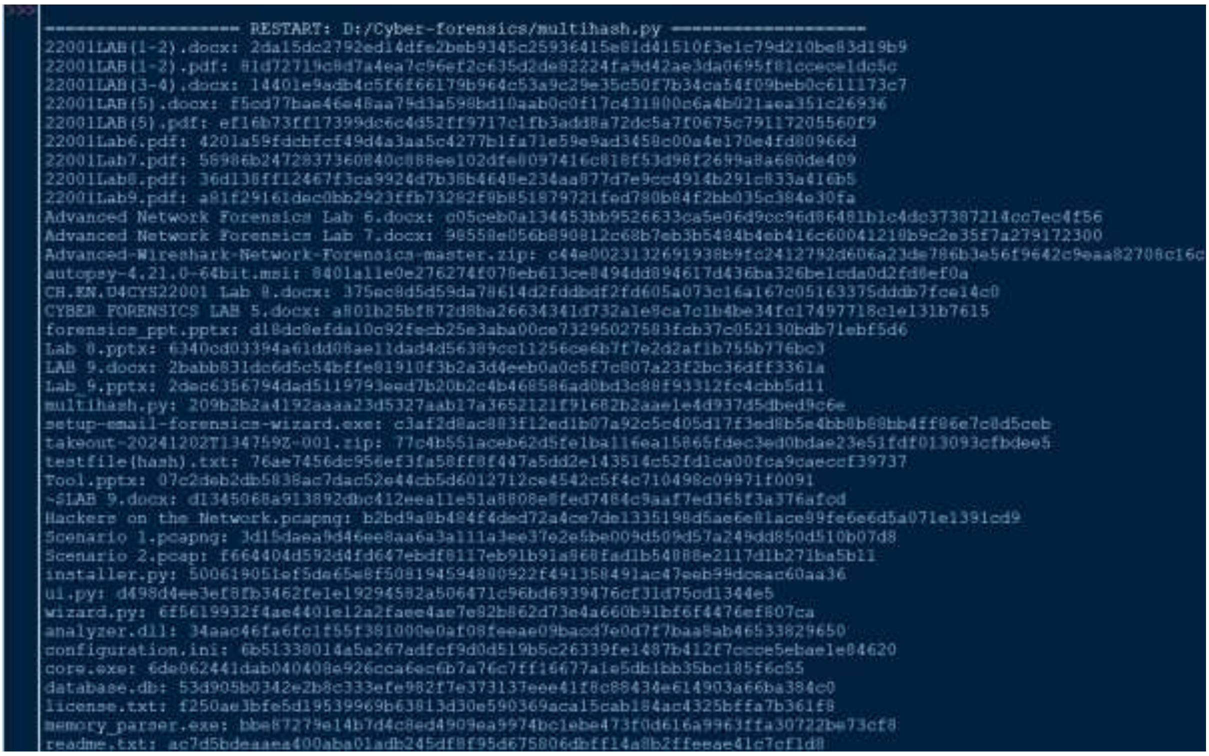
985CCBEF3C0041D949E21B3B71E8977F6E453ACC182EB935

It is proved that the hash value of that file is not same it is modified ok

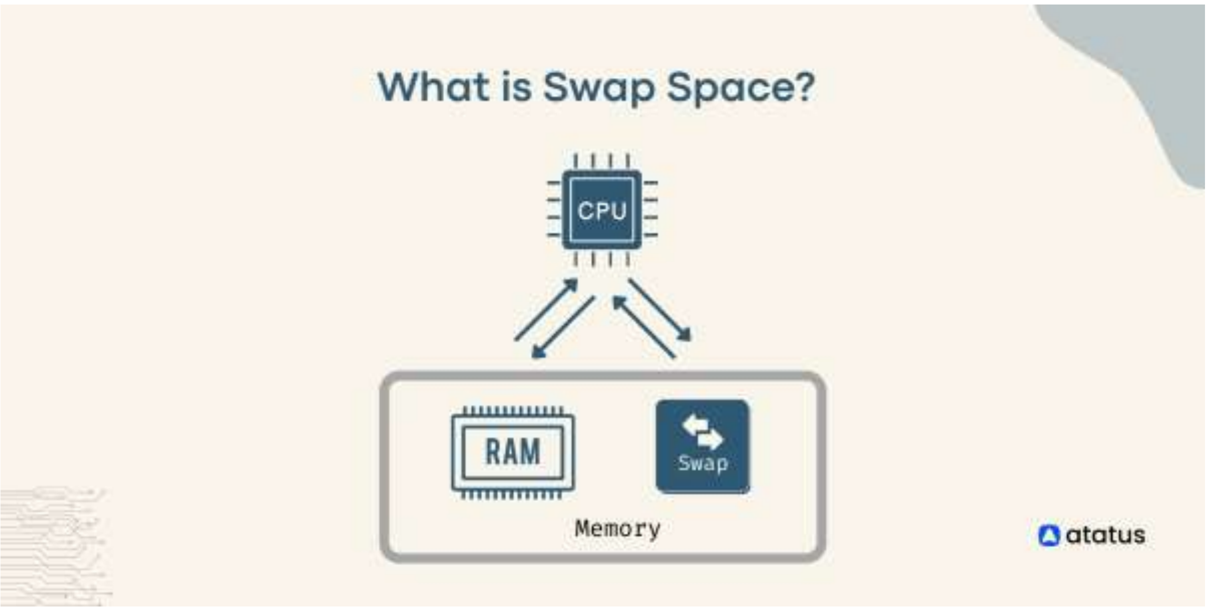
To automate hashing for multiple files:

```
import hashlib
import os
def hash_file(filename, algorithm="sha256"):
    hasher = hashlib.new(algorithm)
    with open(filename, 'rb') as f:
        while chunk := f.read(4096):
            hasher.update(chunk)
    return hasher.hexdigest()
folder_path = f"D:\Cyber-forensics"
for root, _, files in os.walk(folder_path):
    for file in files:
        file_path = os.path.join(root, file)
        print(f"{file}: {hash_file(file_path, 'sha256')}")
```

screenshot:



```
==================== RESTART: D:/Cyber-forensics/multihash.py ====================
22001LAB(1-2).docx: 2da15dc2792ed14dfe2beb9345c25936415e81d41510f3e1c79d210be83d19b9
22001LAB(1-2).pdf: 81d72719c8d7a4ea7c96ef2c635d2de82224fa9d42ae3da0695f81cceceldc5c
22001LAB(3-4).docx: 14401e9adb4c5f6f66179b964c53a9c29e35c50f7b34ca54f09beb0c611173c7
22001LAB(5).docx: f5cd77bae46e48aa79d3a598bd10aab0c0f17c431800c6a4b021aea351c26936
22001LAB(5).pdf: ef16b73ff17399dc6c4d52ff9717c1fb3add8a72dc5a7f0675c79117205560f9
22001Lab6.pdf: 4201a59fdcbfcf49d4a3aa5c4277b1fa71e59e9ad3458c00a4e170e4fd80966d
22001Lab7.pdf: 56986b247283736084 0c888ee102dfe8097416c818f53d98f2699a8a680de409
22001Lab8.pdf: 36d138ff12467f3ca9924d7b38b4648e234aa877d7e9cc4914b291c833a416b5
22001Lab9.pdf: a81f29161dec0bb2923ffb73282f8b851879721fed780b84f2bb035c384e30fa
Advanced Network Forensics Lab 6.docx: c05ceb0a134453bb9526633ca5e06d9cc96d86481b1c4dc37387214cc7ec4f56
Advanced Network Forensics Lab 7.docx: 98558e056b890812c68b7eb3b5484b4eb416c60041218b9c2e35f7a279172300
Advanced-Wireshark-Network-Forensics-master.zip: c44e0023132691938b9fc2412792d606a23de786b3e56f9642c9eaa82708c16c
autopsy-4.21.0-64bit.msi: 8401a11e0e276274f078eb613ce8494dd894617d436ba326be1cda0d2fd8ef0a
CH.EN.U4CYS22001 Lab 8.docx: 375ec8d5d59da78614d2fddbdf2fd605a073c16a167c05163375dddb7fce14c0
CYBER FORENSICS LAB 5.docx: a801b25bf872d8ba26634341d732a1e8ca7c1b4be34fc17497718c1e131b7615
forensics_ppt.pptx: d18dc8efda10c92fecb25e3aba00ce73295027583fcb37c052130bdb71ebf5d6
Lab 8.pptx: 6340cd03394a61dd08ae11dad4d56389cc11256ce6b7f7e2d2af1b755b776bc3
LAB 9.docx: 2babb831dc6d5c54bffe81910f3b2a3d4eeb0a0c5f7c807a23f2bc36dff3361a
Lab_9.pptx: 2dec6356794dad5119793eed7b20b2c4b468586ad0bd3c88f93312fc4cbb5d11
multihash.py: 209b2b2a4192aaaa23d5327aab17a3652121f91682b2aae1e4d937d5dbed9c6e
setup-email-forensics-wizard.exe: c3af2d8ac883f12ed1b07a92c5c405d17f3ed8b5e4bb8b88bb4ff86e7c8d5ceb
takeout-20241202T134759Z-001.zip: 77c4b551aceb62d5fe1ba116ea15865fdec3ed0bdae23e51fdf013093cfbdee5
testfile(hash).txt: 76ae7456dc956ef3fa58ff8f447a5dd2e143514c52fd1ca00fca9caeccf39737
Tool.pptx: 07c2deb2db5838ac7dac52e44cb5d6012712ce4542c5f4c710498c09971f0091
~$LAB 9.docx: d1345068a913892dbc412eea11e51a8808e8fed7484c9aaf7ed365f3a376afcd
Hackers on the Network.pcapng: b2bd9a8b484f4ded72a4ce7de1335198d5ae6e81ace99fe6e6d5a071e1391cd9
Scenario 1.pcapng: 3d15daea9d46ee8aa6a3a111a3ee37e2e5be009d509d57a249dd850d510b07d8
Scenario 2.pcap: f664404d592d4fd647ebdf8117eb91b91a868fad1b54888e2117d1b271ba5b11
installer.py: 500619051ef5de65e8f508194594880922f491358491ac47eeb99dcaac60aa36
ui.py: d498d4ee3ef8fb3462fe1e19294582a506471c96bd6939476cf31d75cd1344e5
wizard.py: 6f5619932f4ae4401e12a2faee4ae7e82b862d73e4a660b91bf6f4476ef807ca
analyzer.dll: 34aac46fa6fc1f55f381000e0af08feeae09bacd7e0d7f7baa8ab46533829650
configuration.ini: 6b51338014a5a267adfcf9d0d519b5c26339fe1487b412f7ccce5ebae1e84620
core.exe: 6de062441dab040408e926cca6ec6b7a76c7ff16677a1e5db1bb35bc185f6c55
database.db: 53d905b0342e2b8c333efe982f7e373137eee41f8c88434e614903a66ba384c0
license.txt: f250ae3bfe5d19539969b63813d30e590369aca15cab184ac4325bffa7b361f8
memory_parser.exe: bbe87279e14b7d4c8ed4909ea9974bc1ebe473f0d616a9963ffa30722be73cf8
readme.txt: ac7d5bdeaaea400aba01adb245df8f95d675806dbff14a8b2ffeeae41c7cf1d8
```



I am using windows so

Here is the steps

For linux try this(Swap Space in Linux)

[https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide- en-US/s1-swap-adding.html](https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/s1-swap-adding.html)

below steps to see the swap space in windows

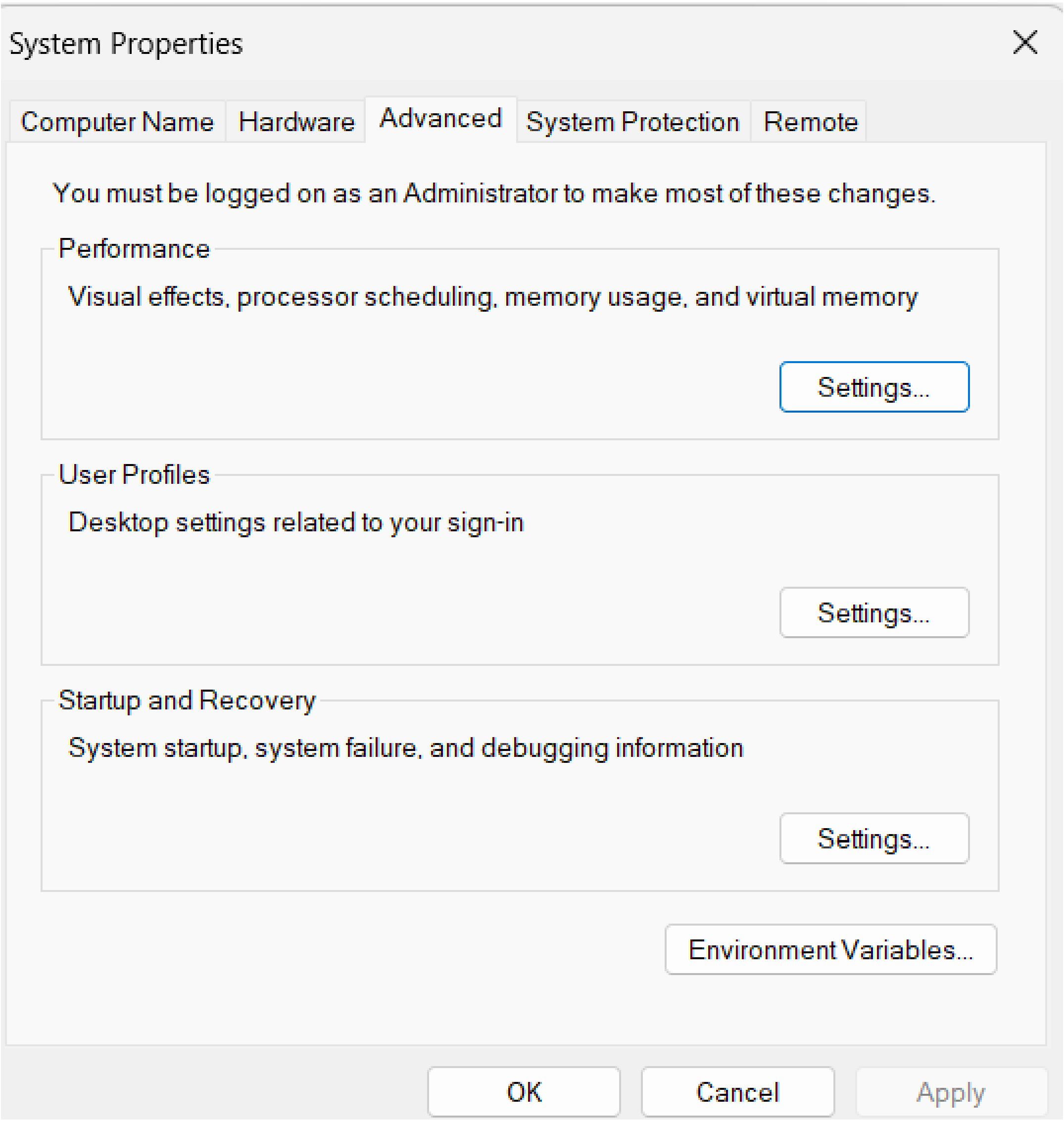
Right-click on "This PC" (or "My Computer") on your desktop and select "Properties".

Access Advanced System Settings:

Click on "Advanced system settings" in the left-hand pane or Just type Advanced system settings

In search.

Click on the "Advanced" tab.



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your sign-in

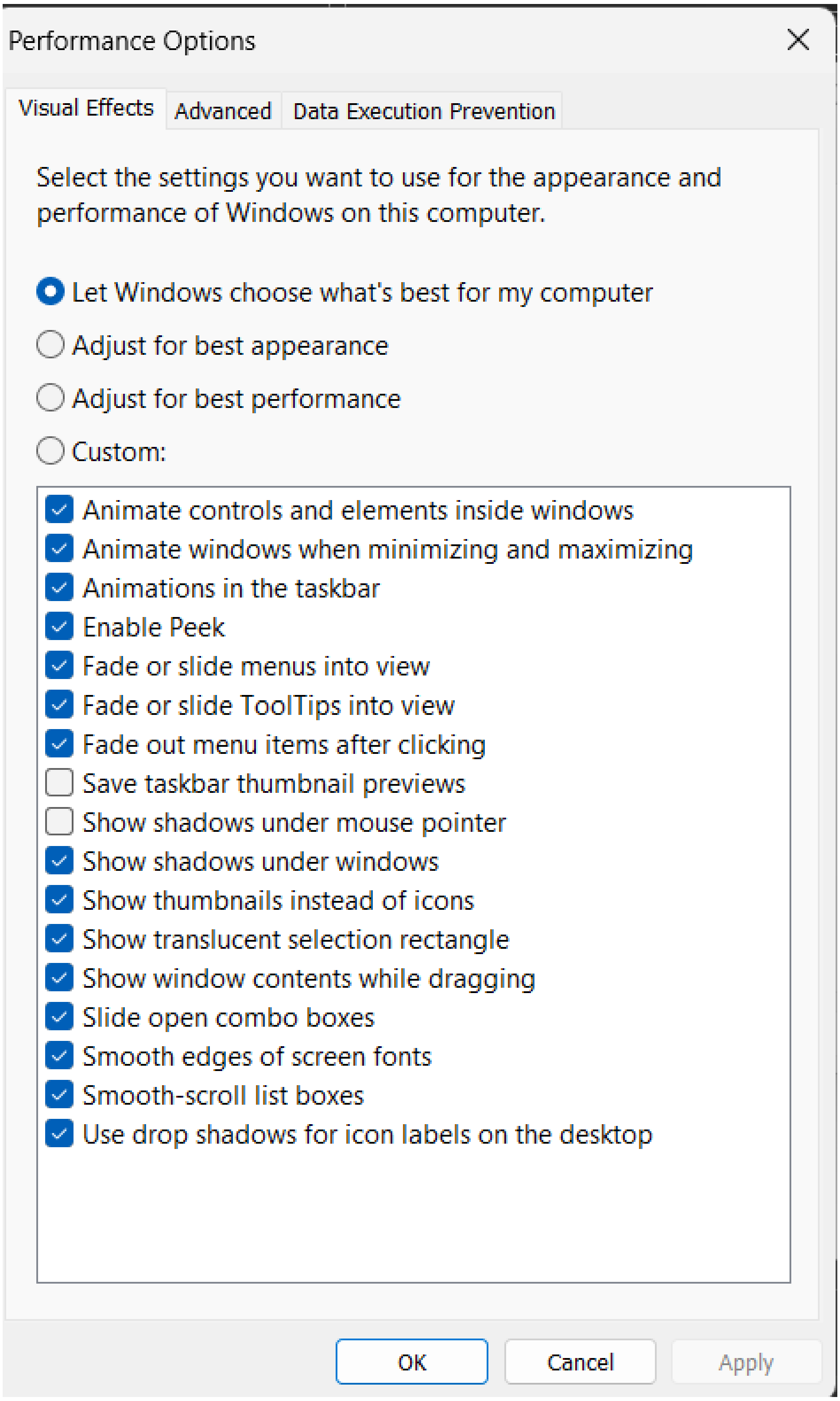
System startup, system failure, and debugging information

2. Access Virtual Memory Settings:

Under the "Performance" section, click "Settings".

Click on the "Advanced" tab.

Click "Change" under "Virtual memory".



Select the settings you want to use for the appearance and performance of Windows on this computer.

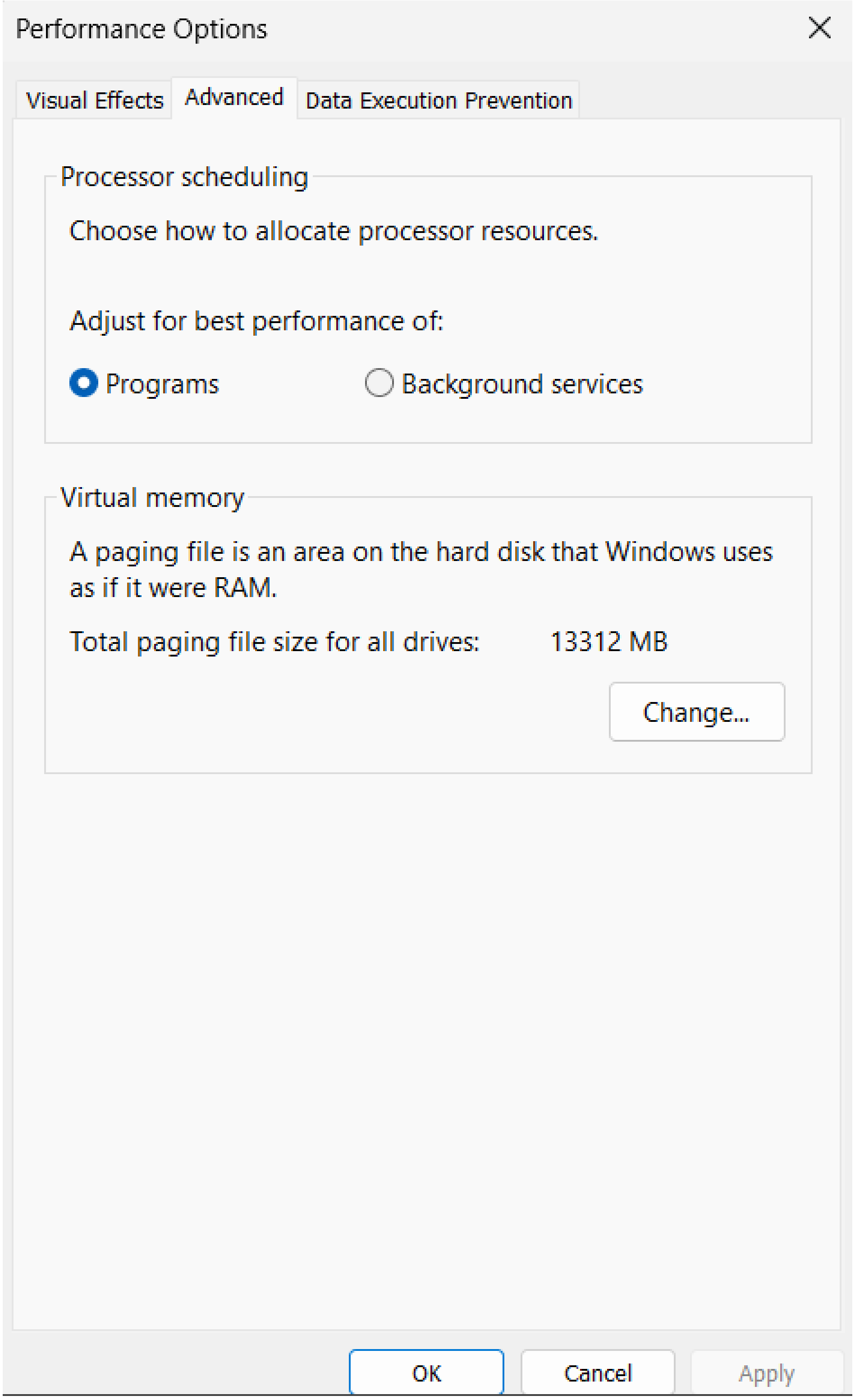
● Let Windows choose what's best for my computer

○ Adjust for best appearance

○ Adjust for best performance

○ Custom:

- ☑ Animate controls and elements inside windows
- ☑ Animate windows when minimizing and maximizing
- ☑ Animations in the taskbar
- ☑ Enable Peek
- ☑ Fade or slide menus into view
- ☑ Fade or slide ToolTips into view
- ☑ Fade out menu items after clicking
- □ Save taskbar thumbnail previews
- □ Show shadows under mouse pointer
- ☑ Show shadows under windows
- ☑ Show thumbnails instead of icons
- ☑ Show translucent selection rectangle
- ☑ Show window contents while dragging
- ☑ Slide open combo boxes
- ☑ Smooth edges of screen fonts
- ☑ Smooth-scroll list boxes
- ☑ Use drop shadows for icon labels on the desktop



Processor scheduling

Choose how to allocate processor resources.

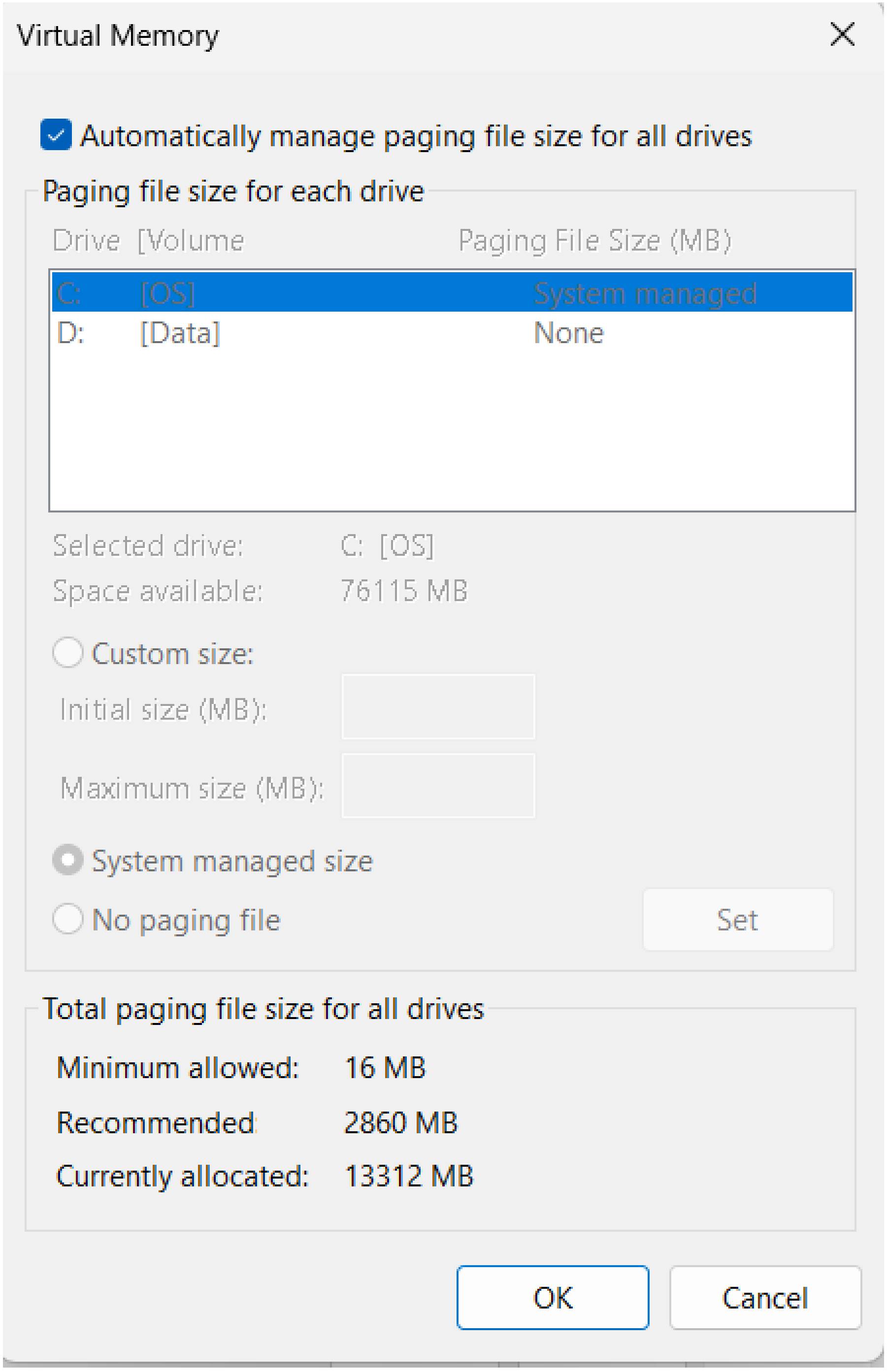
Adjust for best performance of:

● Programs ○ Background services

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 13312 MB



☑ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume		Paging File Size (MB)
C:	[OS]	System managed
D:	[Data]	None

Selected drive: C: [OS]

Space available: 76115 MB

○ Custom size:

Initial size (MB):

Maximum size (MB):

● System managed size

○ No paging file

Total paging file size for all drives

Minimum allowed: 16 MB

Recommended 2860 MB

Currently allocated: 13312 MB

3. Configure Virtual Memory:

Uncheck the box labeled "Automatically manage paging file size for all drives".

Select the drive where you want to store the pagefile (usually the drive where Windows is installed).

Choose "Custom size".

Set the new size:

Initial Size: Enter the desired initial size in MB.

Maximum Size: Enter the desired maximum size in MB.

If you have 8 gb ram for initial value set it has 8gb=1.5x8192=12288 MB.

For maximum size is

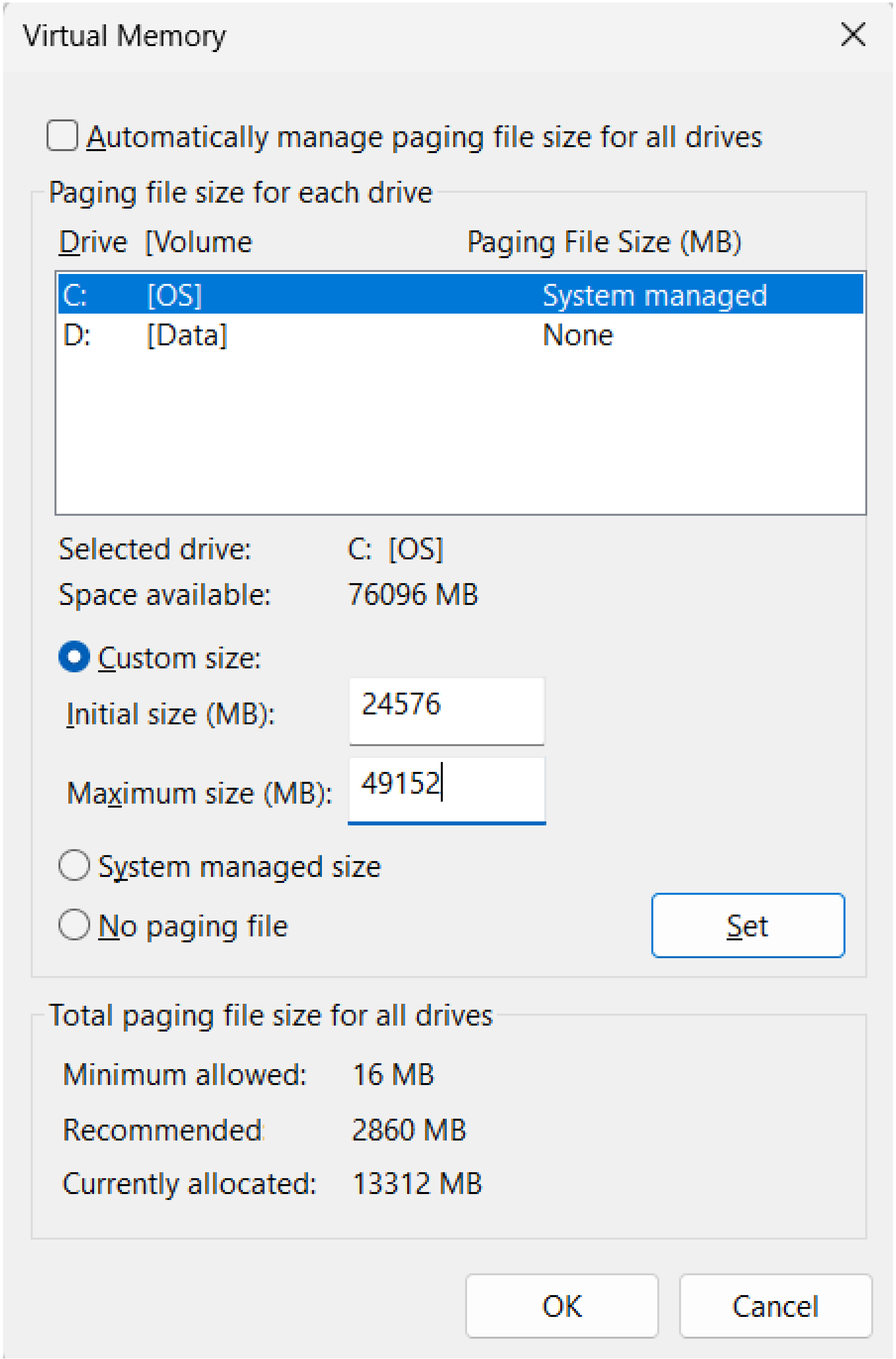
8gb=3x8192=24576 MB.

If you have 16 gb ram for initial value set it has 16gb=1.5x16384= 24576 MB.

For maximum size is

16gb=3x 16384= 49152 MB.

Click "Set" and then "OK" to apply the changes.



Virtual Memory

☐ Automatically manage paging file size for all drives

Paging file size for each drive

Drive	[Volume	Paging File Size (MB)
C:	[OS]	System managed
D:	[Data]	None

Selected drive: C: [OS]

Space available: 76096 MB

● Custom size:

Initial size (MB): 24576

Maximum size (MB): 49152

○ System managed size

○ No paging file

Total paging file size for all drives

Minimum allowed: 16 MB

Recommended: 2860 MB

Currently allocated: 13312 MB

Restart your computer: The changes will take effect after restarting your computer.

Important Considerations:

Pagefile Size:

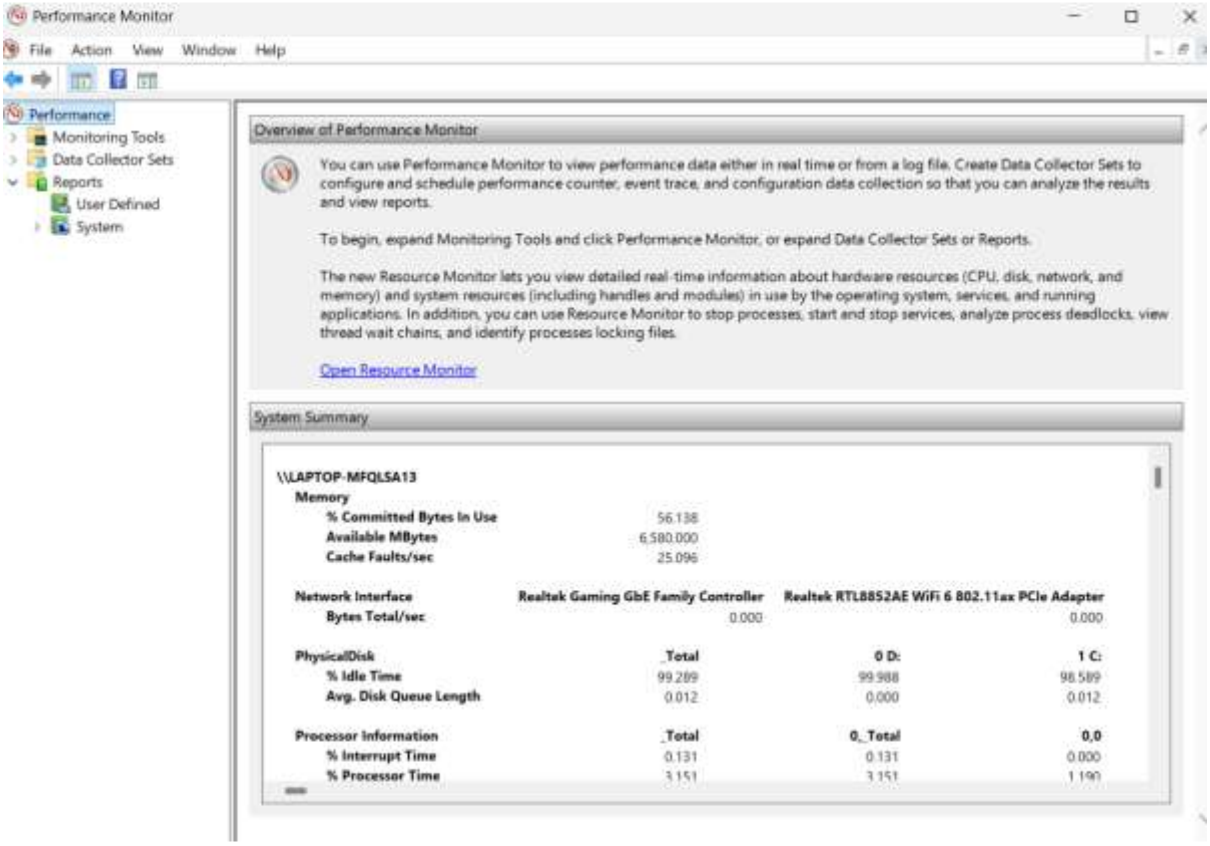
A good starting point for the pagefile size is often 1.5 to 2 times the amount of your RAM, but you can adjust it based on your needs and the type of applications you use.

SSD vs. HDD:

If you have an SSD (Solid State Drive), it's generally recommended to keep the pagefile size smaller, as the SSD is faster than a traditional HDD (Hard Disk Drive).

Monitoring Pagefile Usage:

You can monitor the pagefile usage using Performance Monitor (type perfmon in the Run window).



You can use Performance Monitor to view performance data either in real time or from a log file. Create Data Collector Sets to configure and schedule performance counter, event trace, and configuration data collection so that you can analyze the results and view reports.

To begin, expand Monitoring Tools and click Performance Monitor, or expand Data Collector Sets or Reports.

The new Resource Monitor lets you view detailed real-time information about hardware resources (CPU, disk, network, and memory) and system resources (including handles and modules) in use by the operating system, services, and running applications. In addition, you can use Resource Monitor to stop processes, start and stop services, analyze process deadlocks, view thread wait chains, and identify processes locking files.

Open Resource Monitor

```
\\LAPTOP-MFQLSA13
  Memory
      % Committed Bytes In Use           56.138
      Available MBytes                6,580.000
      Cache Faults/sec                   25.096

  Network Interface       Realtek Gaming GbE Family Controller   Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
      Bytes Total/sec                                  0.000                                            0.000

  PhysicalDisk                           _Total                0 D:                1 C:
      % Idle Time                        99.289              99.988              98.589
      Avg. Disk Queue Length              0.012               0.000               0.012

  Processor Information                  _Total             0,_Total                0,0
      % Interrupt Time                    0.131               0.131               0.000
      % Processor Time                    3.151               3.151               1.190
```