Cyber Forensics Lab - 9

Name: R. Subramanian
Roll No: CH.EN.U4CYS22043
Lab Topic: Volatility Framework and Memory Forensics

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

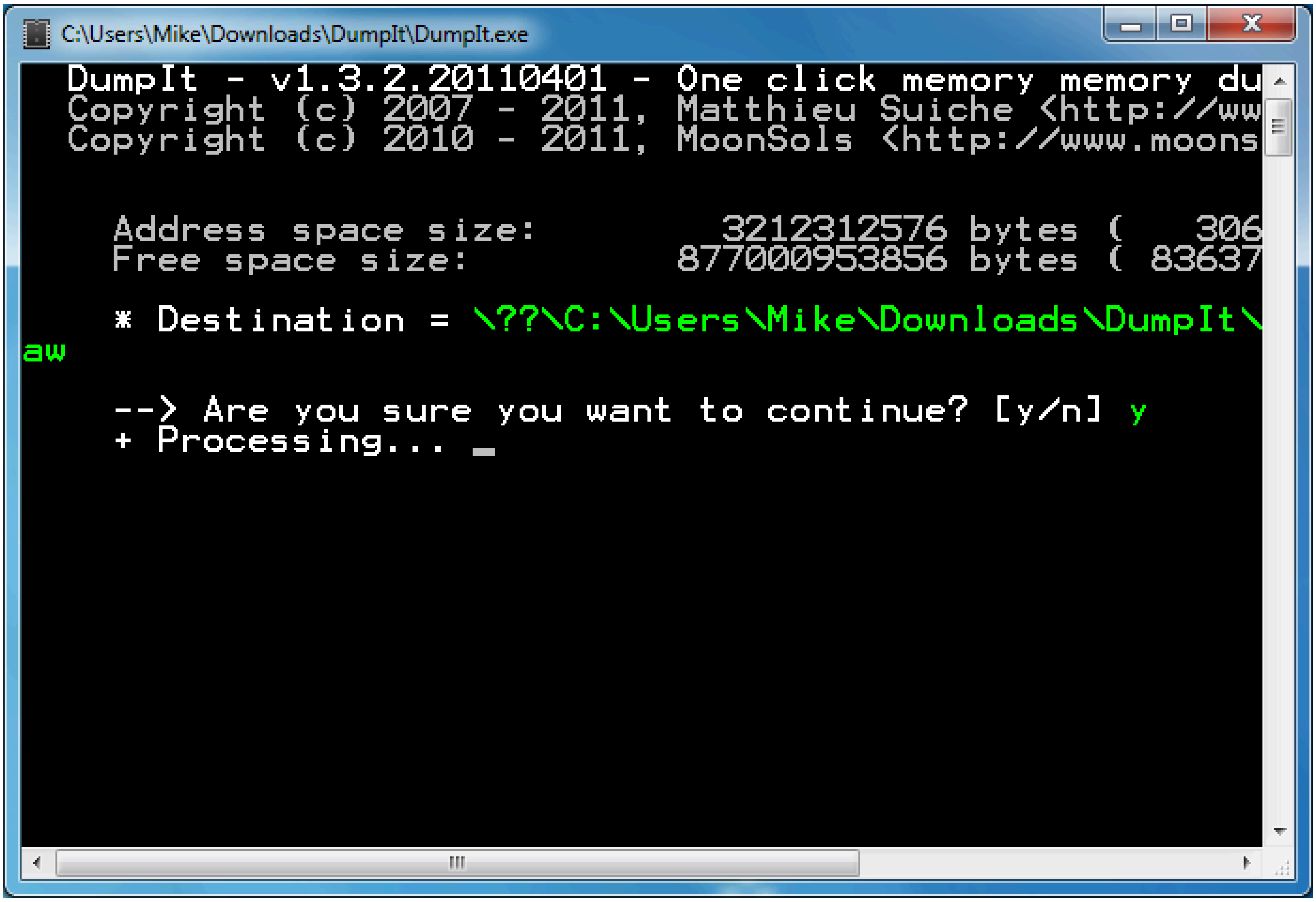
Overview:

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:



C:\Users\Mike\Downloads\DumpIt\DumpIt.exe

```
  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
  ```

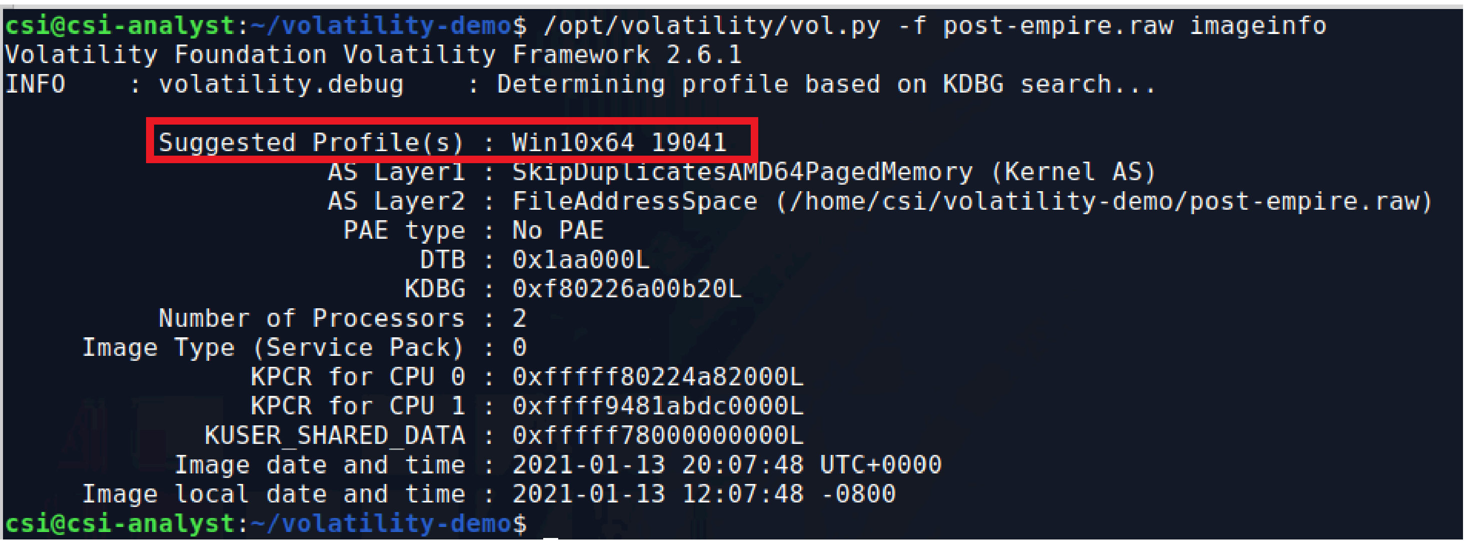
- Check loaded DLLs:

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

- Analyze registry hives:

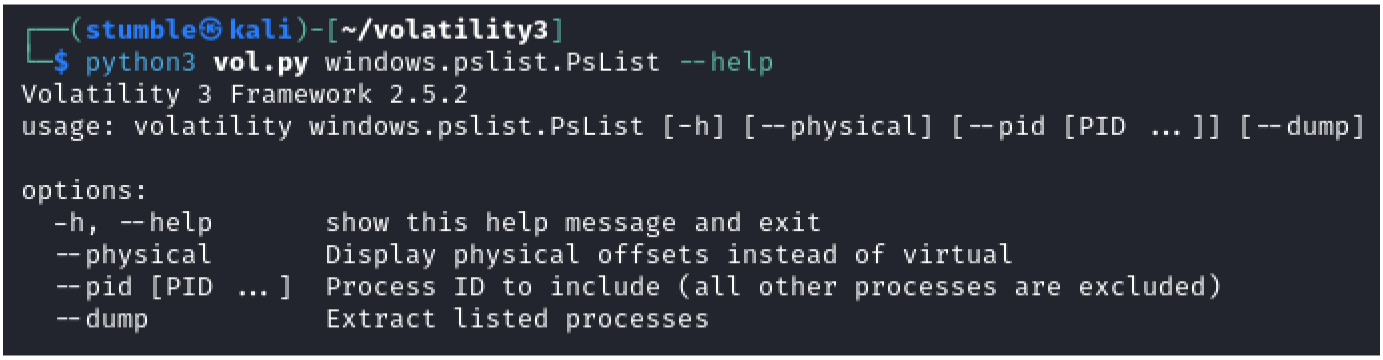
  ```
  python3 vol.py -f memory.raw windows.registry.hivelist
  ```

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

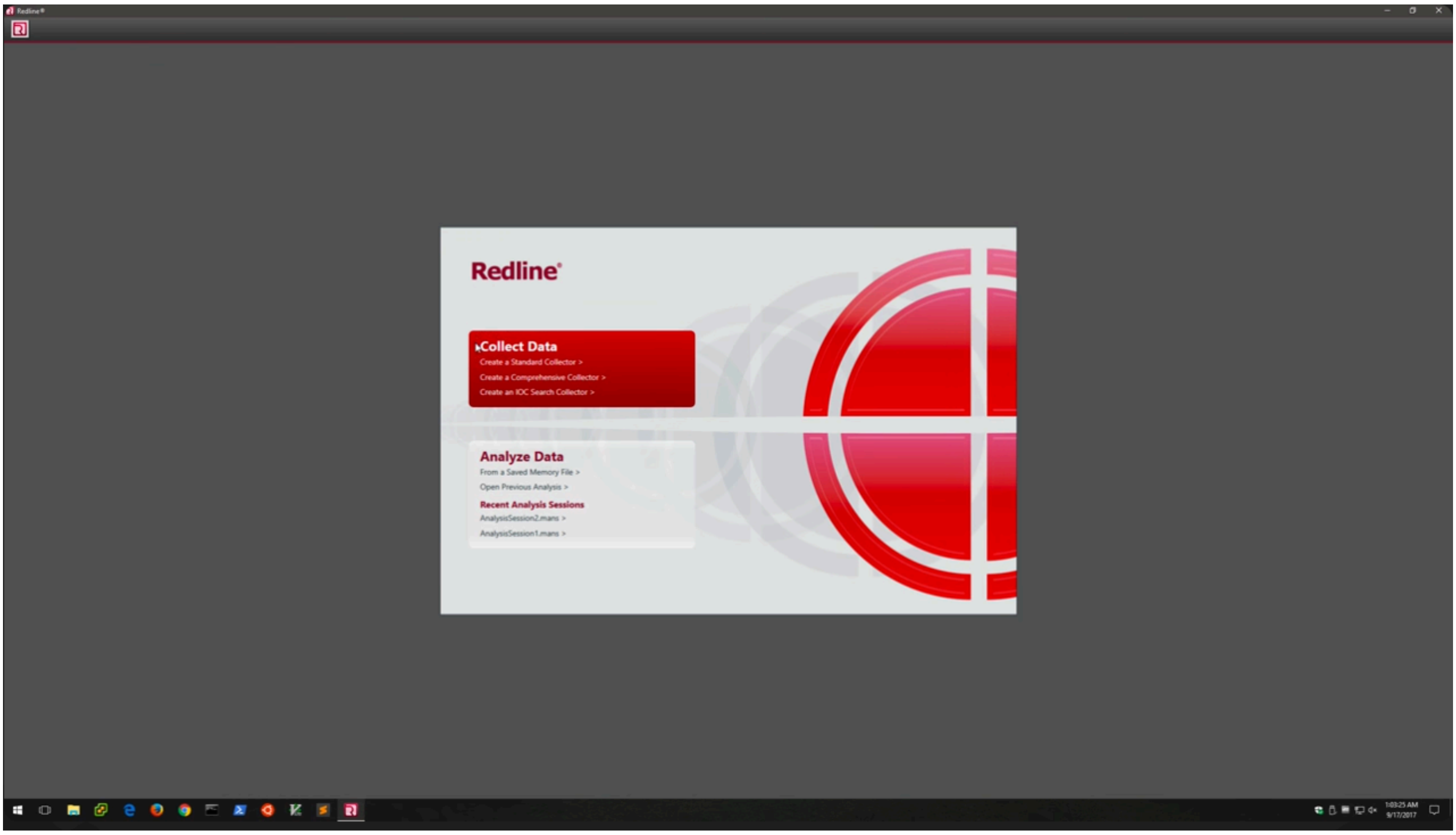
Overview:

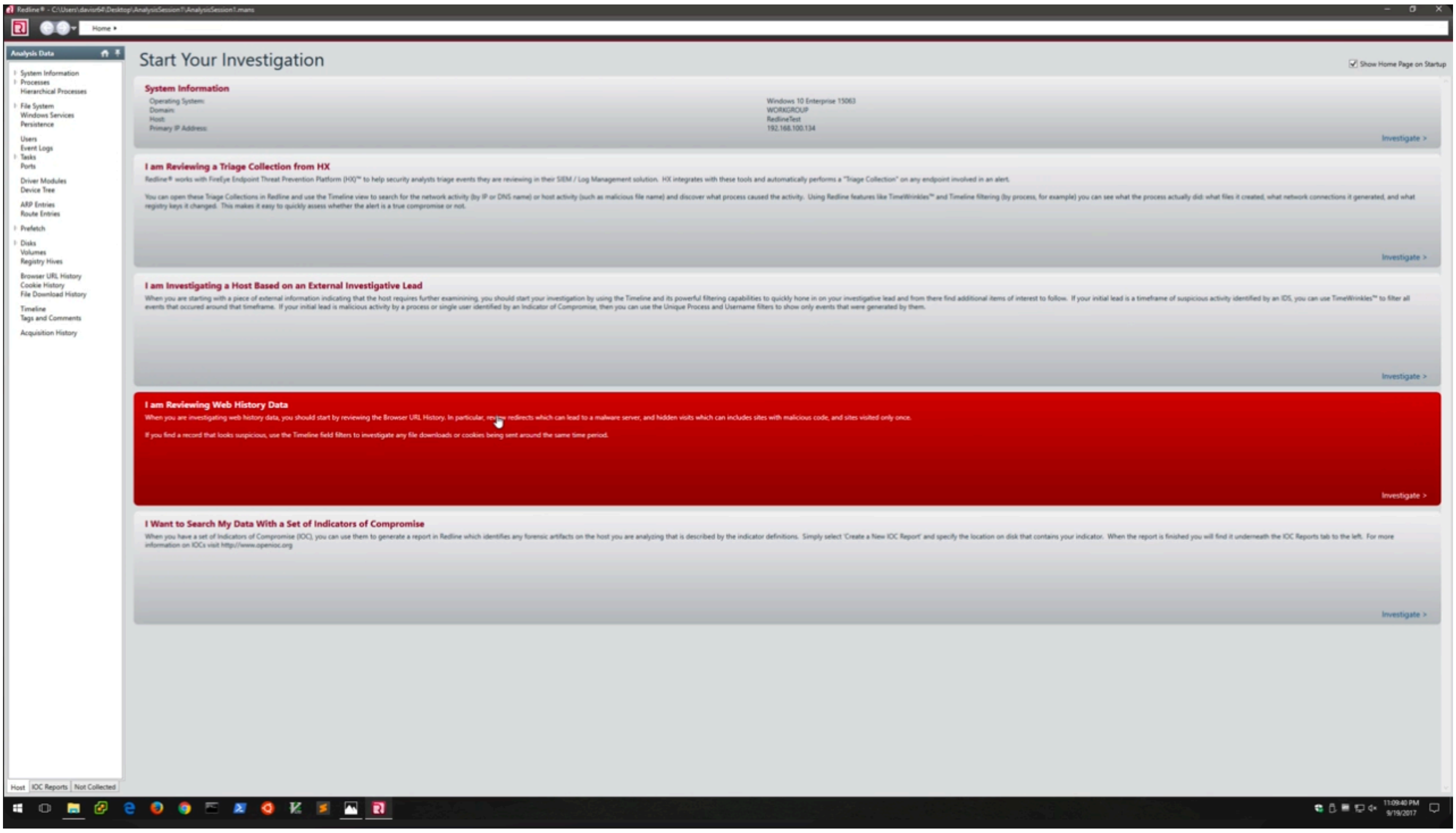
FireEye **Redline** provides a user-friendly interface for analyzing forensic artifacts, especially useful for those preferring a graphical approach.

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

☑ Show Home Page on Startup

System Information

Operating System: Windows 10 Enterprise 15063
Domain: WORKGROUP
Host: RedlineTest
Primary IP Address: 192.168.100.134

I am Reviewing a Triage Collection from HX

Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.

You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.

I am Investigating a Host Based on an External Investigative Lead

When you are starting with a piece of external information indicating that the host requires further examinining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occured around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

I am Reviewing Web History Data

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

I Want to Search My Data With a Set of Indicators of Compromise

When you have a set of Indicators of Compromise (IOC), you can use them to generate a report in Redline which identifies any forensic artifacts on the host you are analyzing that is described by the indicator definitions. Simply select 'Create a New IOC Report' and specify the location on disk that contains your indicator. When the report is finished you will find it underneath the IOC Reports tab to the left. For more information on IOCs visit http://www.openioc.org

Extracting Slack Space using WinHex

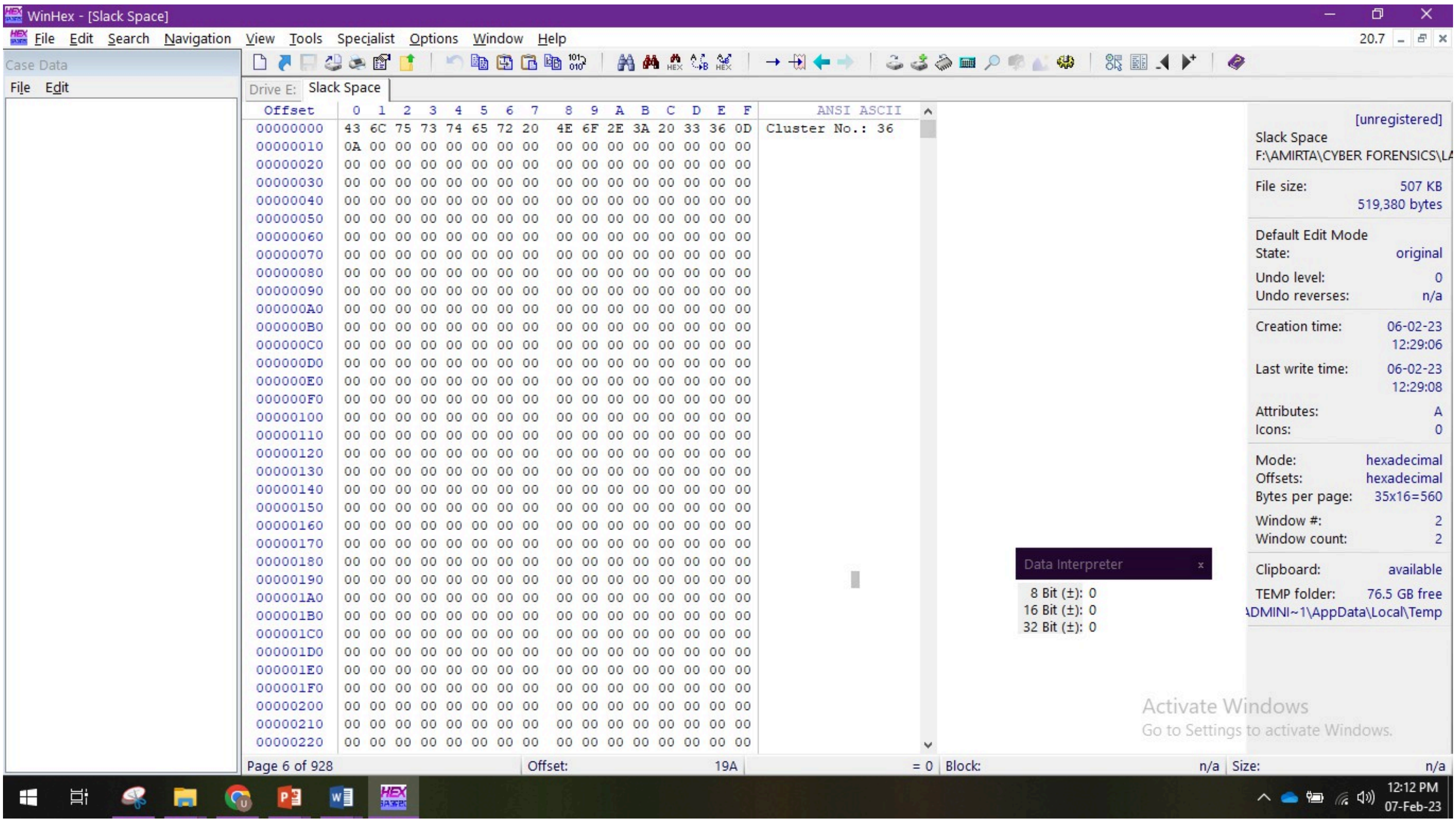
WinHex can extract slack space from:

- Any kind of file, including binary files.
- Hard disks, floppy disks, CD-ROMs, DVDs.
- Smart media, compact flash, memory sticks.
- All other drive types accessible in Windows.
- Even your computer's RAM!

More Info: [Slack Space Definition]

Steps to Extract Slack Space

1. **Install WinHex**
2. **Go to Tools**
3. **Target your Drive**
4. **Find Slack Space**



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  43 6C 75 73 74 65 72 20  4E 6F 2E 3A 20 33 36 0D   Cluster No.: 36
00000010  0A 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

```
 8 Bit (±): 0
16 Bit (±): 0
32 Bit (±): 0
```

```
[unregistered]
Slack Space
F:\AMIRTA\CYBER FORENSICS\LA
File size:            507 KB
                519,380 bytes
Default Edit Mode
State:              original
Undo level:                0
Undo reverses:           n/a
Creation time:      06-02-23
                    12:29:06
Last write time:    06-02-23
                    12:29:08
Attributes:                A
Icons:                     0
Mode:            hexadecimal
Offsets:         hexadecimal
Bytes per page:    35x16=560
Window #:                  2
Window count:              2
Clipboard:         available
TEMP folder:    76.5 GB free
DMINI~1\AppData\Local\Temp
```

```
Page 6 of 928 | Offset: 19A | = 0 | Block: n/a | Size: n/a
```

Compute Hash

1. Try various **hash functions** for a particular file or folder.
2. Alter that file or folder.
3. Recheck the hash and **prove that there has been a modification**.

(Insert Screenshot of Hash Computation Here)

Swap Space in Linux

More Info: Adding Swap Space in Linux

Adding Swap Space in Linux

It is necessary to add more swap space after installation, especially for memory-intensive operations.

Steps to Add Swap Space

1. Disable swapping for the associated logical volume:

```
swapoff -v /dev/VolGroup00/LogVol01
```

2. Resize the LVM2 logical volume by 256 MB:

```
lvm lvresize /dev/VolGroup00/LogVol01 -L +256M
```

3. Format the new swap space:

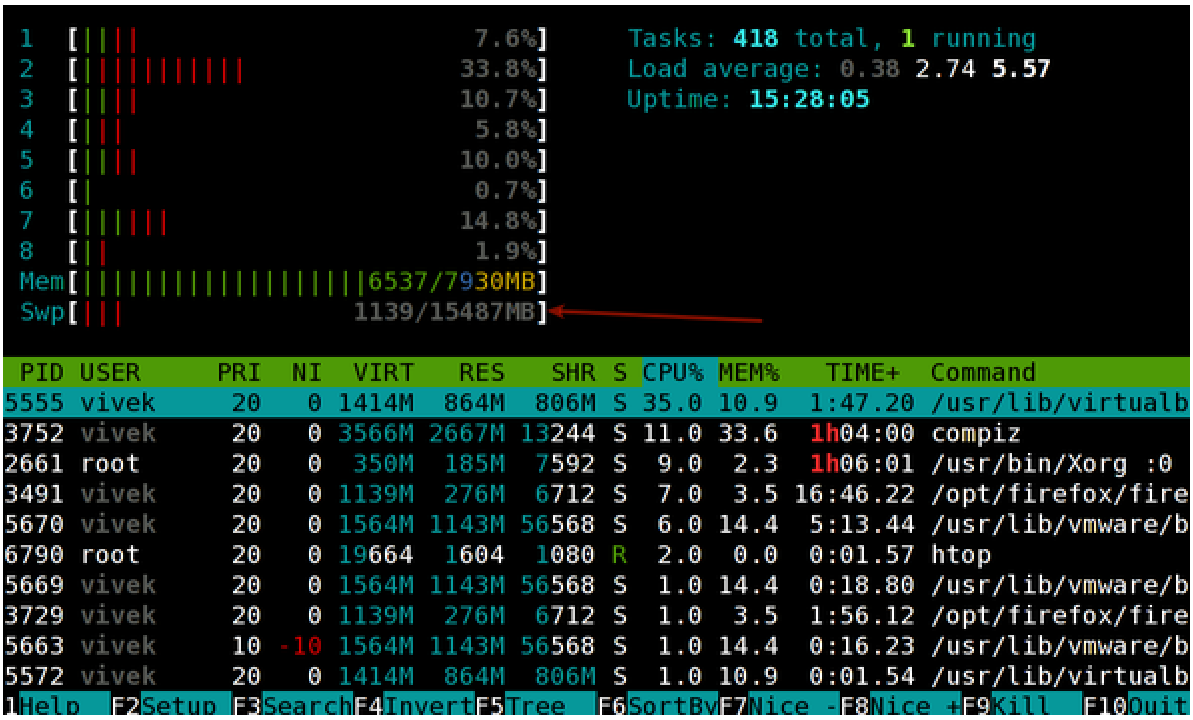
```
mkswap /dev/VolGroup00/LogVol01
```

4. Enable the extended logical volume:

```
swapon -va
```

5. Test that the logical volume has been extended properly:

```
cat /proc/swaps
free
```



```
  1  [||||                     7.6%]     Tasks: 418 total, 1 running
  2  [|||||||||||             33.8%]     Load average: 0.38 2.74 5.57
  3  [||||                    10.7%]     Uptime: 15:28:05
  4  [|||                      5.8%]
  5  [||||                    10.0%]
  6  [|                        0.7%]
  7  [||||||                  14.8%]
  8  [||                       1.9%]
  Mem[||||||||||||||||||6537/7930MB]
  Swp[|||            1139/15487MB]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
5555 vivek      20   0 1414M  864M  806M S 35.0 10.9  1:47.20 /usr/lib/virtualb
3752 vivek      20   0 3566M 2667M 13244 S 11.0 33.6  1h04:00 compiz
2661 root       20   0  350M  185M  7592 S  9.0  2.3  1h06:01 /usr/bin/Xorg :0
3491 vivek      20   0 1139M  276M  6712 S  7.0  3.5 16:46.22 /opt/firefox/fire
5670 vivek      20   0 1564M 1143M 56568 S  6.0 14.4  5:13.44 /usr/lib/vmware/b
6790 root       20   0 19664  1604  1080 R  2.0  0.0  0:01.57 htop
5669 vivek      20   0 1564M 1143M 56568 S  1.0 14.4  0:18.80 /usr/lib/vmware/b
3729 vivek      20   0 1139M  276M  6712 S  1.0  3.5  1:56.12 /opt/firefox/fire
5663 vivek      10 -10 1564M 1143M 56568 S  1.0 14.4  0:16.23 /usr/lib/vmware/b
5572 vivek      20   0 1414M  864M  806M S  1.0 10.9  0:01.54 /usr/lib/virtualb
F1Help  F2Setup F3SearchF4InvertF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

Swap Space in Windows

Steps to Configure Virtual Memory in Windows

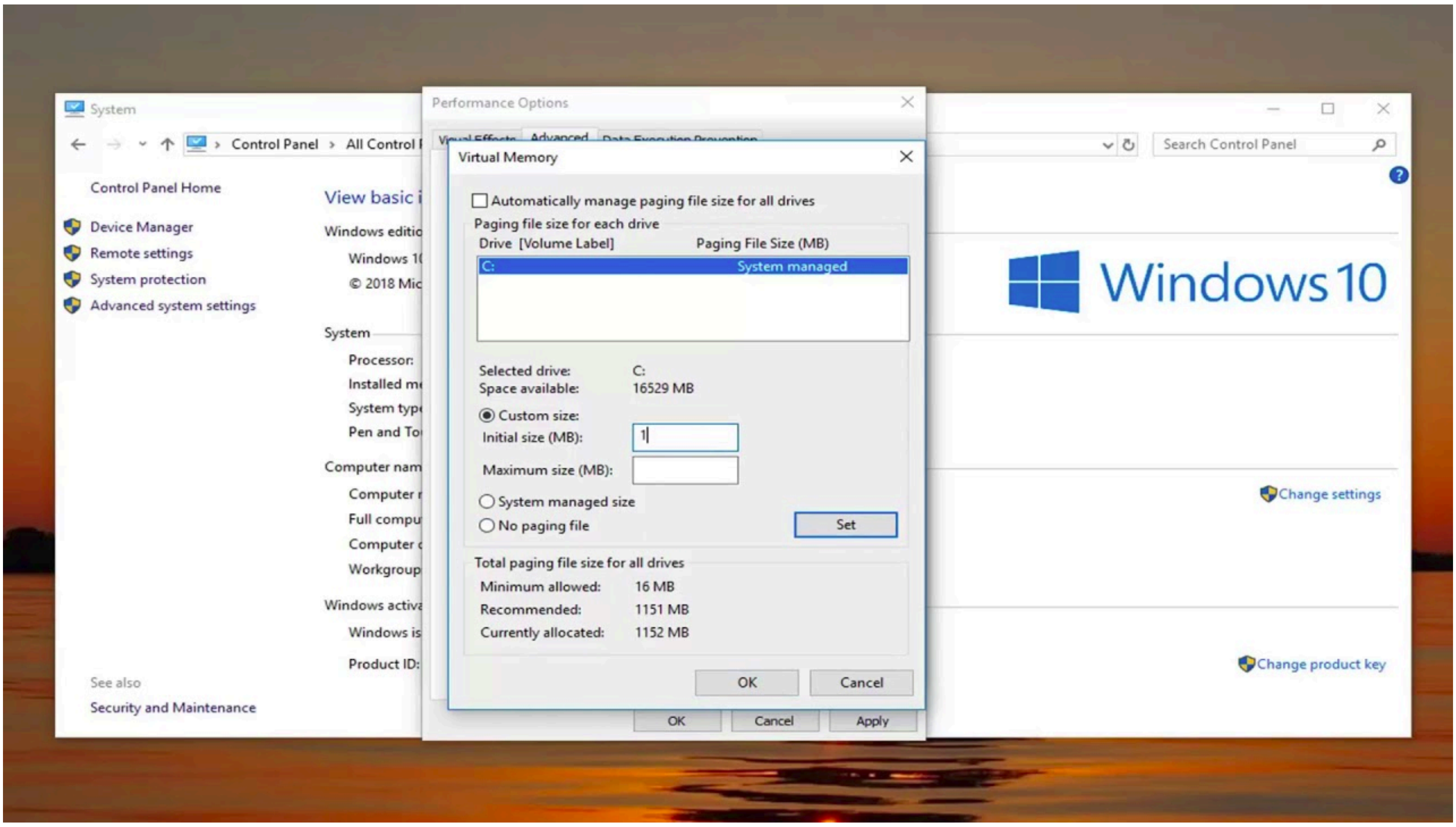
1. **Right-click on "This PC" (or "My Computer")** on your desktop and select **"Properties"**.
2. Access Advanced System Settings:
   - Click on **"Advanced system settings"** in the left-hand pane.
   - Click on the **"Advanced"** tab.
3. Access Virtual Memory Settings:
   - Under **"Performance"** section, click **"Settings"**.
   - Click on the **"Advanced"** tab.

- Click **"Change"** under **"Virtual memory"**.

4. 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.
    - Click **"Set"** and then **"OK"** to apply the changes.
5. **Restart your computer** for the changes to take effect.

Important Considerations:

- **Pagefile Size:** A good starting point is **1.5 to 2 times** the amount of your RAM.
- **SSD vs. HDD:** If using an **SSD**, keep the pagefile **smaller** as SSDs are faster than HDDs.
- **Monitoring Pagefile Usage:** Use **Performance Monitor** (`perfmon` in Run window) to track usage.



Virtual Memory

☐ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	System managed

Selected drive: C:
Space available: 16529 MB

● Custom size:
Initial size (MB): 1
Maximum size (MB):
○ System managed size
○ No paging file

Total paging file size for all drives
Minimum allowed: 16 MB
Recommended: 1151 MB
Currently allocated: 1152 MB

Conclusion

This lab covered essential forensic tools such as **DumpIt, Volatility 3, Redline, and WinHex**, focusing on **memory forensics, slack space extraction, and swap space management**. These skills are critical for **digital forensics investigations**.