

Lab 7

Windows Memory Diagnostics

ITSC205: Operating Systems Internals

NAME: Ahmed Almass

Table of Contents

[Lab Outcome(s) 2](#_Toc472777602)

[Reading 2](#_Toc472777603)

[Introduction 2](#_Toc472777604)

[1.0 Memory Information and Settings 3](#_Toc472777605)

[2.0 Memory Analysis with System Internals tools 6](#_Toc472777606)

|  |  |  |
| --- | --- | --- |
| Examine Memory Information and Settings | 15 |  |
| Memory Analysis with System Internals Tools | 15 |  |
| TOTAL MARK | 30 |  |

Lab Outcome(s)

* Examine Windows memory settings.
* Examine Windows memory management techniques.
* Analyze memory behavior of normal system operations.

Reading

* Textbook sections Windows chapter -21.3.5.2 ( Virtual Memory Manager)

Introduction

Memory is where all the magic happens, all the code and data to be executed resides in physical memory. Evidence of compromise may never be written to disk but memory has a high potential to contain malicious code in whole or in part. A victimized system will contain evidence that system resources were used by an attack.

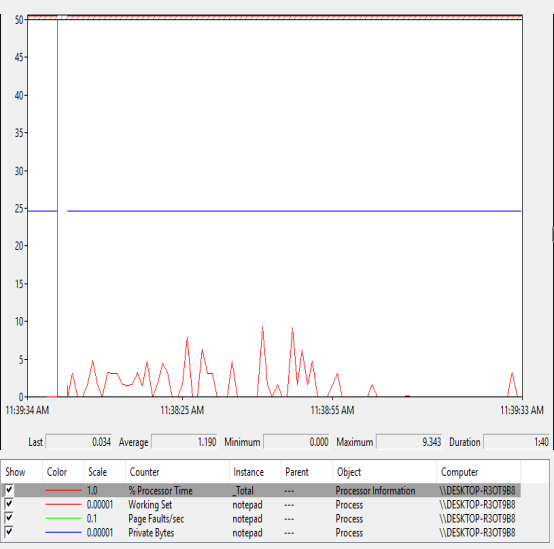
In this lab, we study important tools that are available to monitor, control, and debug memory usage in Windows.

1. Memory Information and Settings \_\_\_/15
2. Use the Windows System Information tool to record the following values (including units):

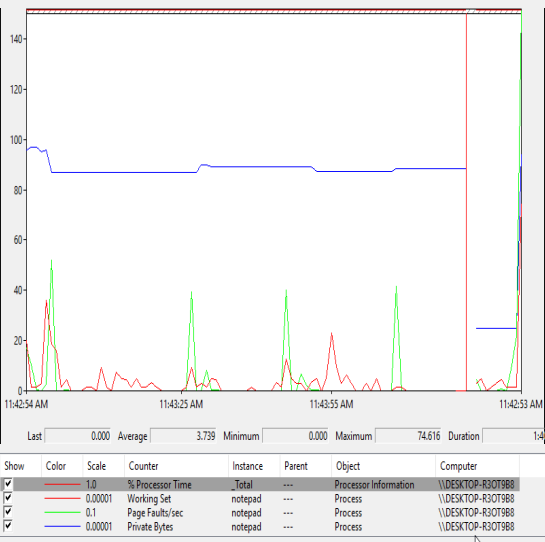
|  |  |
| --- | --- |
| *Physical Memory* | *Virtual Memory* |
| Total 11.1GB | Total 13.4 GB |
| Available 9.82 GB | Available 12.3 GB |

1. Use performance monitor to analyze memory usage per process
2. Start notepad process.
3. Add a counter and select **process** object
4. Under instances, select Notepad instance.
5. On the counters list, **select** the following counters and explain each one. Check the box “Show description” and write down the description of each of the following:
   * 1. Page faults: its when a thread refers to a virtual memory page that not in its working set in main memory. This possible can cause the page to be fetched from disk if its on the standby list and hence already memory, or if it is in use by another process with whom the page is shared.
     2. Pool Nonpaged Bytes : is the size, in bytes, of the nonpaged pool, an area of the system virtual memory that is used for object that cannot be written to disk, but must remain in physical memory as long as they are allocated.
     3. Pool Paged Bytes: is the size, in bytes, of the paged pool, an area of the system virtual memory that is used for object that can be written to disk.
     4. Private Bytes: amount of byes of memory that is process has allocated that cannot be shared with other process.
     5. Working Set: is the current size, of the working set of this process. The working set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the working set of the process even if they are not in use. When free memory falls below a threshold, pages are trimmed from working sets. If they are needed they will then be soft-faulted back into the working set before leaving main memory.
6. Select page fault, working set and private bytes only for notepad process. After adding these counters analyze the graph and results. Use notepad (type something and try to save the file). Analyze the process page faults and working set changes. Demonstrate and explain the results to the instructor

Before:



After typing & saving:



1. Start Task manager and add the following columns: Working set, page faults. Write down the working set size for notepad process. If each page is 4KB how many pages are in used (working set) by notepad process?

PID cpu WorkingSet-Mem private Page-fault



1. Demo and explain to the instructor which process has the highest working set and which process has the highest page faults and why?

Highest working-set: SearchUI



Highest Page-fault:



|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |

Start the Performance Monitor tool. Add a new counter and select Memory Object. Change the vertical scale maximum on the graph to 1000. Add the following counters and create some activity in the system to see the memory performance while running different process (you can start notepad and access different web sites with animation).

1. Select the following memory features and answer the questions .You can find the definitions by checking the show description box.
   1. What is commit limit?

Is the amount of virtual memory that can be committed without having to extent the paging files. It is measured in bytes. Committed memory is the physical memory which has space reserved on the disk paging files. There can be one paging file on each logical drive. If the pagng files are be expanded, this limit increases accordingly. This counter displays the last observed value only; it is not an average.

* 1. Demand Zero Faults/sec. What are zeroed pages?

Demand Zero Faults/sec is the rate at which a zeroed page is required to satisfy the fault.

Zeroed pages: pages emptied of previously stored data and filled with zeros, are a security feature of windows that prevent processes from seeing data stored by earlier processes that used the memory spaced

* 1. What is **Modified Page** List Bytes?

The amount of physical memory, in bytes that is assigned to the modified page list. This memory contains cached data and code that is not actively in use by processes, the system and the system cache. This memory needs to be written out before it will be available for allocation to a process or for system use.

* 1. Page Faults. What is the difference between **soft fault** and **hard fault**?

Page Fault/sec: is the average number of pages faulted per second.

Hard Fault: those that require disk access

Soft Fault: where the faulted page is found elsewhere in physical memory

* 1. What is the difference between Pool Paged Allocs and Pool Nonpaged Allocs ?

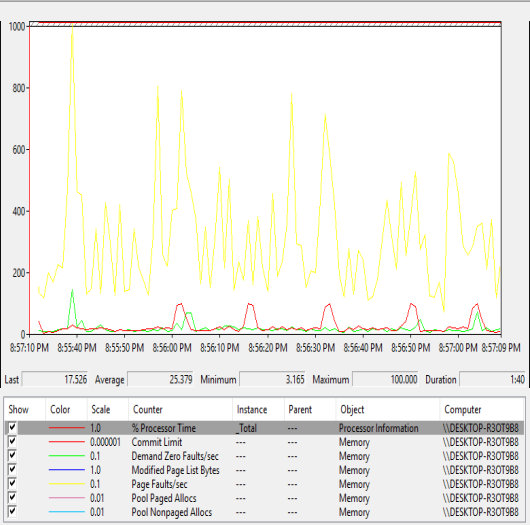
Pool Paged Allocs: is the number of calls to allocate space in the paged pool. The paged pool is an area of the system virtual memory that is used for objects that can be written to disk when they are not being used.

Pool Nonpaged Allocs: is the numbers of calls to allocate space in the nonpaged pool. The nonpaged pool is an area of system memory area for objects that cannot be written to disk and must remain in physical memory as long as they are allocated.

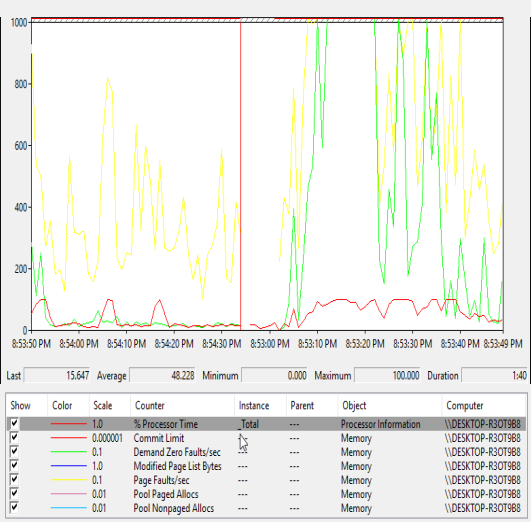
Both is measured in numbers of calls to allocate space regardless of the amount of space allocated in each call .

1. Add memory counters and start some process that uses lots of memory and analyze its memory usage. Demo the results to the instructor

Before processes:



With processes:



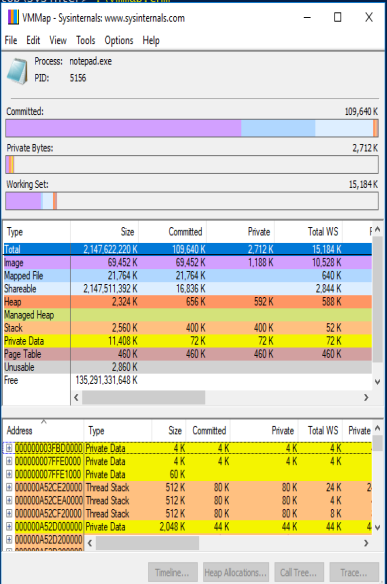
|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |

1. Memory Analysis with System Internals tools \_\_\_/15

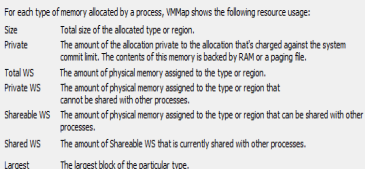
**A. Vmmap utility**

The VMMap utility from Sysinternals can show you a detailed view of the virtual memory being utilized by any process on your machine, divided into categories for each type of allocation.

1. Start notepad or a Web browser process.
2. Run Vmmap utility from System Internals Suite directory.
3. To analyze virtual memory of notepad process , click on File > Select process and select notepad or any other process that you want to analyze



1. Click on Help > Quick help to find the definition of each column or category of this utility
2. Demo and explain to the instructor the different memory sections allocated to this process. Analyze base addresses, sizes, permissions , working set ,

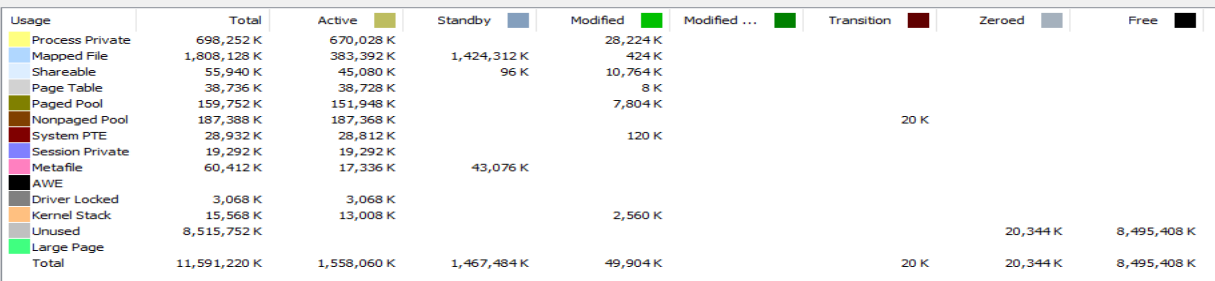


|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |

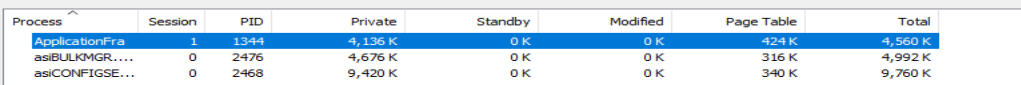
**B. RAMMap**

The movement of pages from process working set to the modified page list and then to the standby page list can also be observed with the Sysinternals tools RAMMap .

1. From system Internals suite , start RAMMap tool
2. Click on use count TAB and observe the usage of different page states



1. Select the processes TAB and analyze the usage of standby, modified pages and page table per process



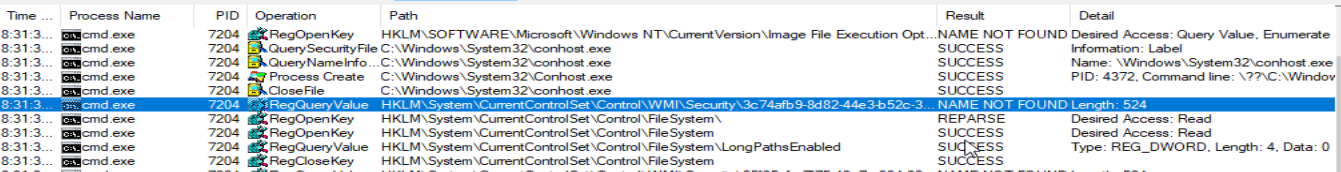
1. Select Physical Pages TAB. Analyze one process ( firefox , vmware or notepad )and demo to the instructor the virtual address , the respective physical address , the offset and the page state of the process.

|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |

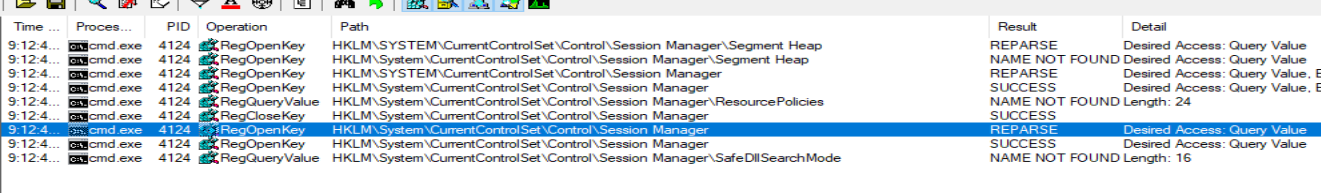
C. PROCMON to Analyze Memory

* Run PROCMON from the Windows Explorer.
* Stop capturing system events.
* Clear the event list.
* Reset the filter.
* Start capturing system events.
* Start CMD.
* Stop capturing system events.
* Find (Ctrl-F) a CMD.EXE event in the list (examine the "Process Name" column), Right-click and include the **process name** in the filter. Now, only events dealing with the CMD process should be shown.





* From the "Path" column, find a prefetch event in the list. Right-click and include the **path** in the filter. Now, only events dealing with prefetching the CMD process should be shown.



**Demonstrate** the results to the instructor. **Explain** the prefetch operations.

Purpose of prefetching: stores specific data about the application that you start up in order to help them start faster. Its stored in windows registry

|  |  |
| --- | --- |
| **ASK THE INSTRUCTOR TO SIGN OFF** |  |