Lab – Processes and Virtual Memory

**Tools**

* Process Explorer from SysInternals OR
* Process Hacker 2

**Instructions**

Execute the sample program given to you then answer the following questions. When finished, press “CTRL-C” to terminate the process.

1. The program allocates memory at a virtual address of **0xca0000**:
   1. What is the size of this allocation?
   2. What are the permissions?
   3. What is the status (or type)? What does that mean?
   4. What is the value written at the beginning of this allocation?
   5. What would a call to *VirtualAlloc* look like to make this memory allocation?
2. The program allocates memory at a virtual address of **0xab0000:**
   1. What are the permissions? How can a program use that differently than the previous allocation?
   2. Why can you not inspect the content of this memory allocation?
   3. What would a call to *VirtualAlloc* look like to make this memory allocation?
3. There is another allocation that has RWX permissions:
   1. What does it appear that this allocation is used for?
4. What handles does this program have open? Describe the importance of each one (or speculate if it’s not clear why the program has that handle).

**Deliverable**

Turn in a Word Document or PDF with answers to the lab questions.