Lab # 2 — Assessment Worksheet

**Course Name and Number: IAM302**

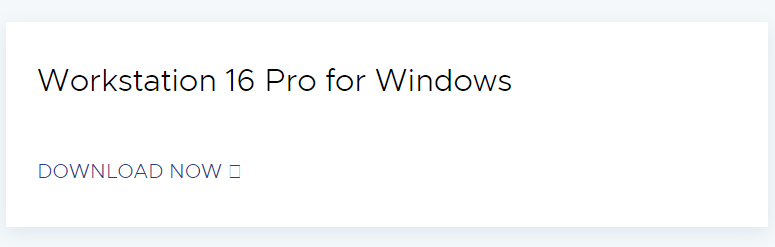
**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Vu Duc Ly**

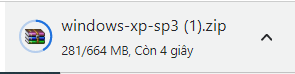
## **Installing Virtual Machine and basic dynamic analysis tool**

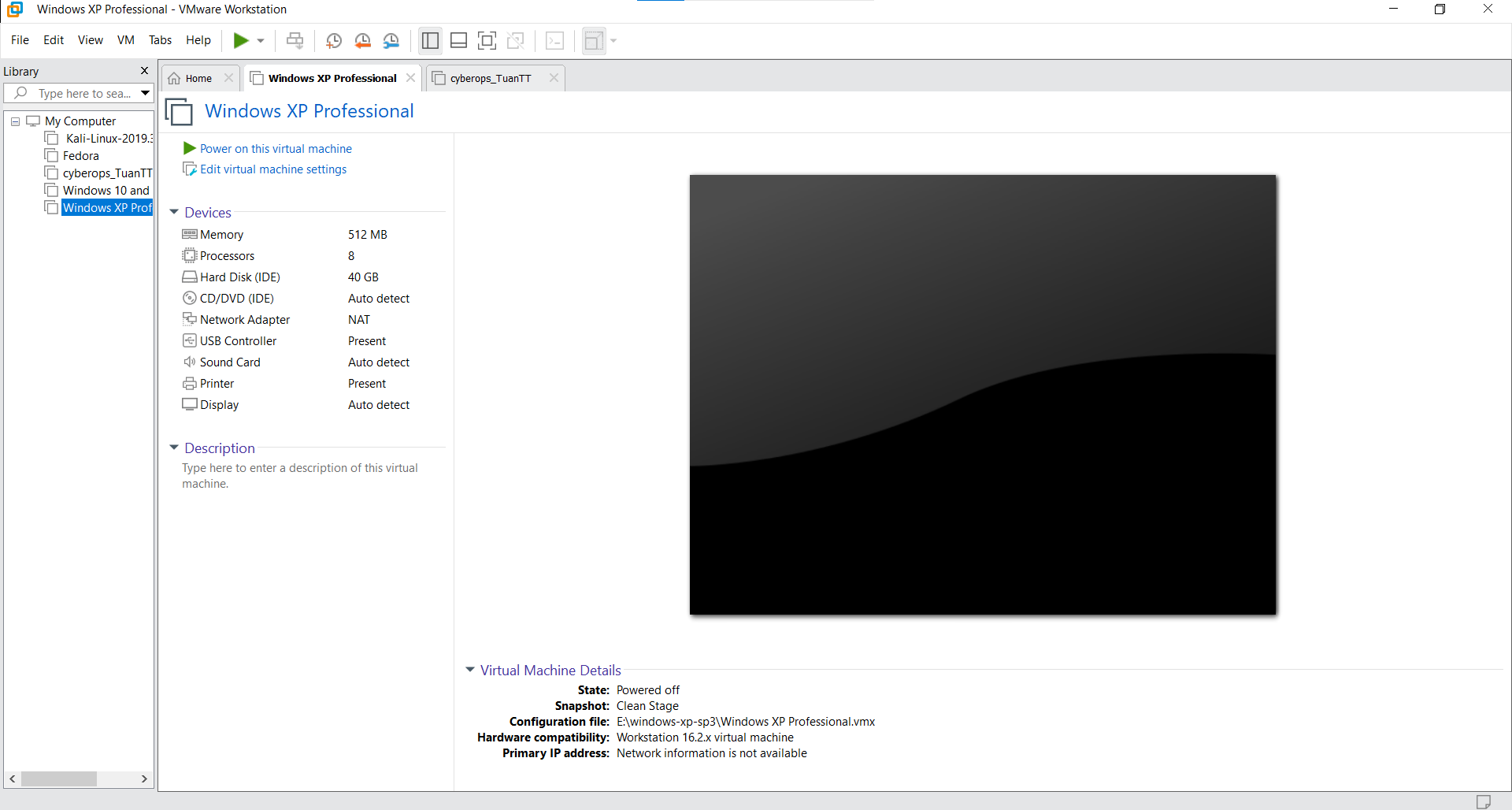
***Installing VMWare***



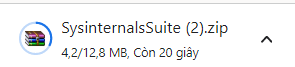


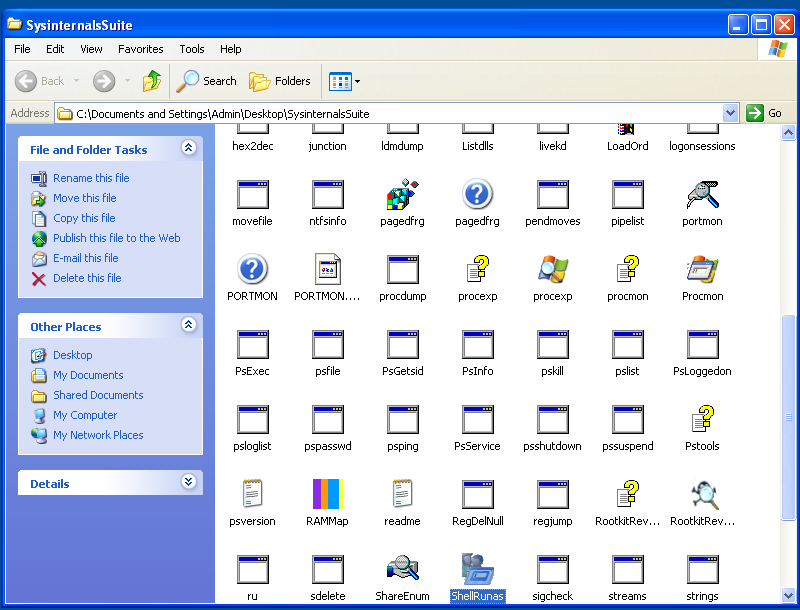
***Installing Windows XP***



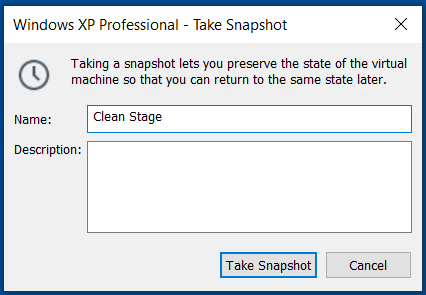


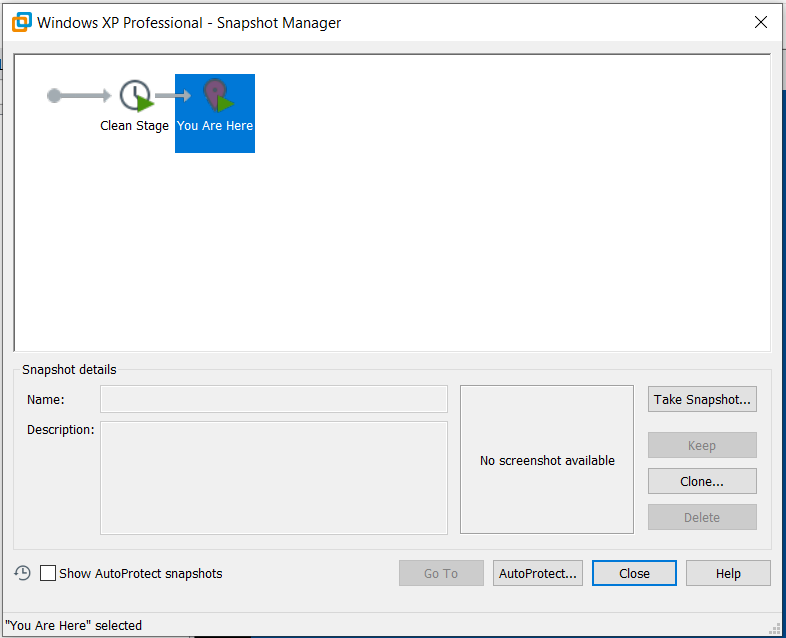
***Installing Process Monitor and Process Explorer***



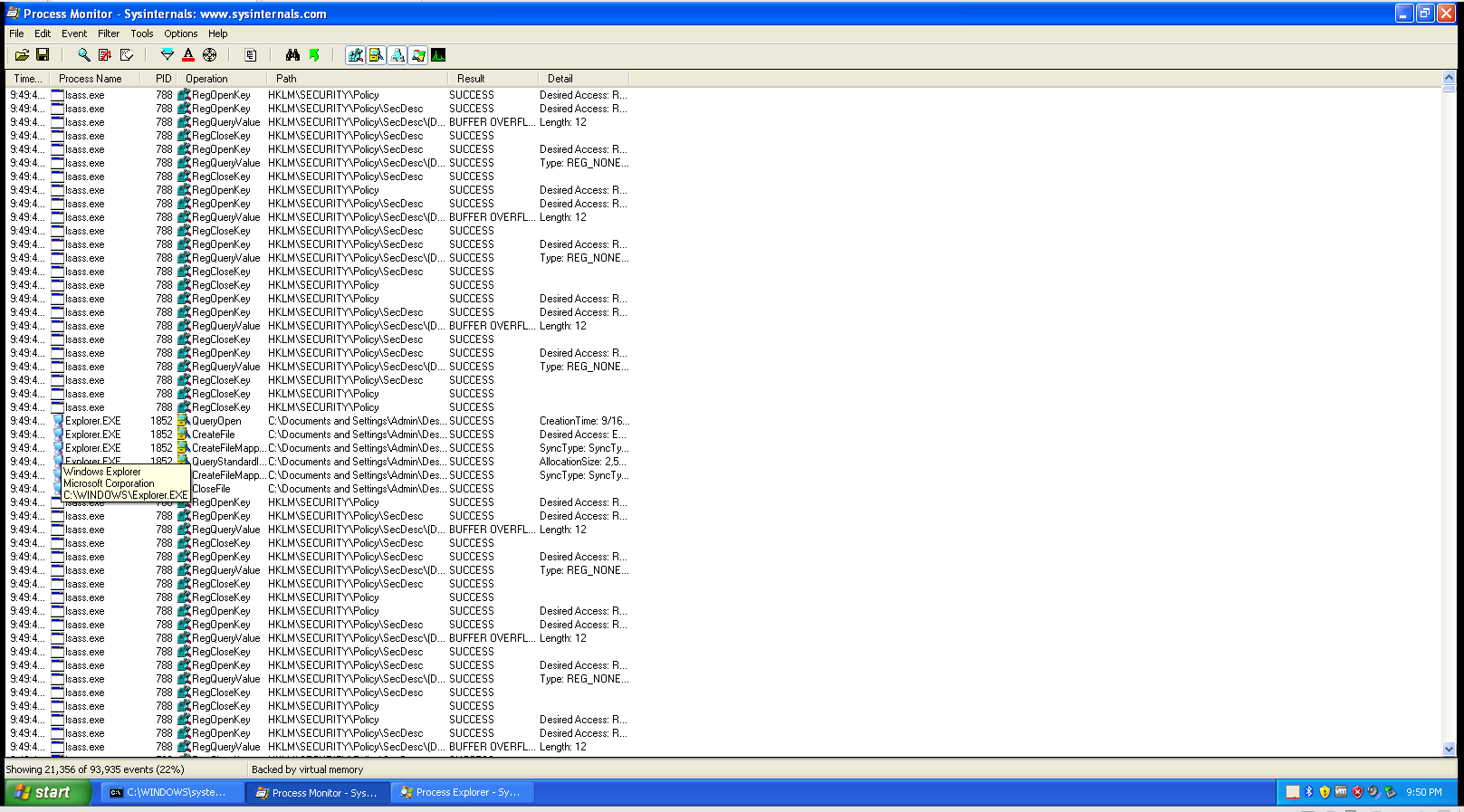


***Take Snapshot Before Running Malware***

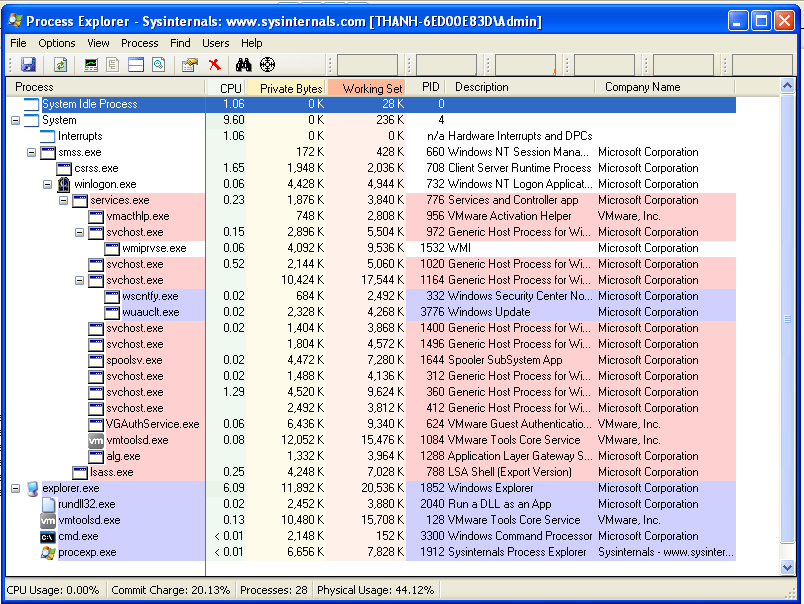




***Running Process Monitor Before Running Malware***



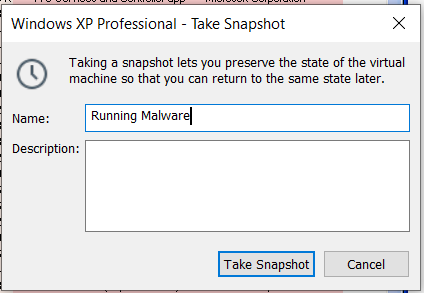
***Running Process Explorer Before Running Malware***

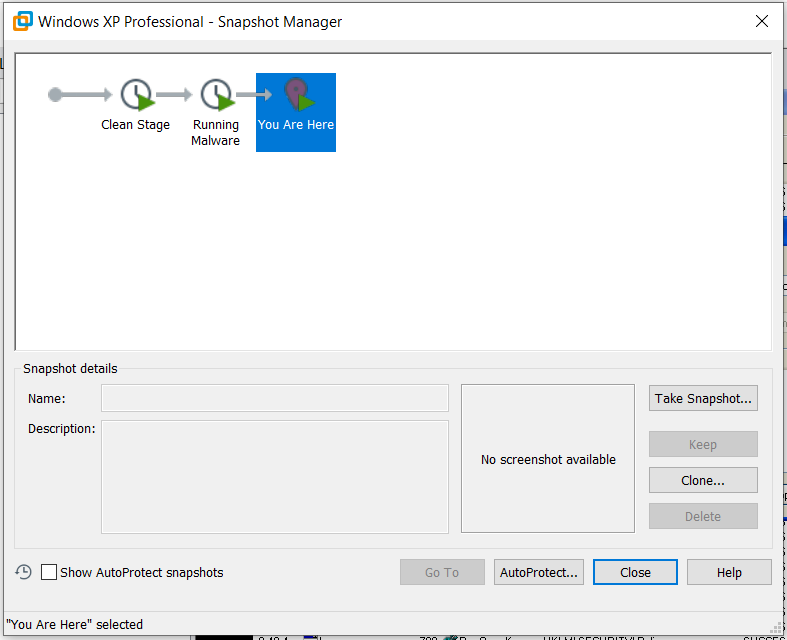


***Running Malware***

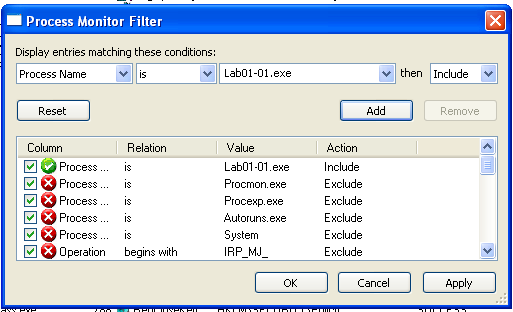


***Take Snapshot After Running Malware***

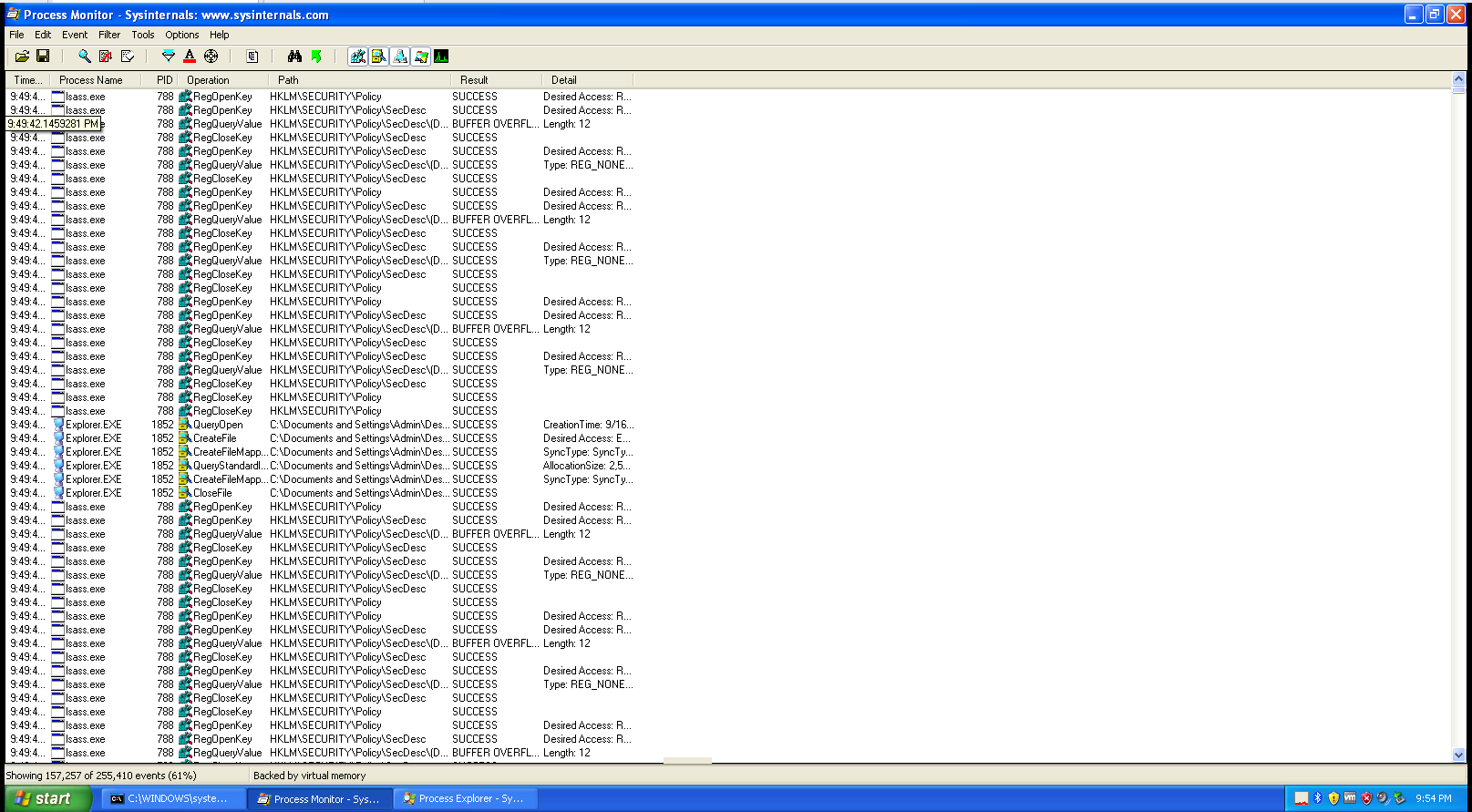




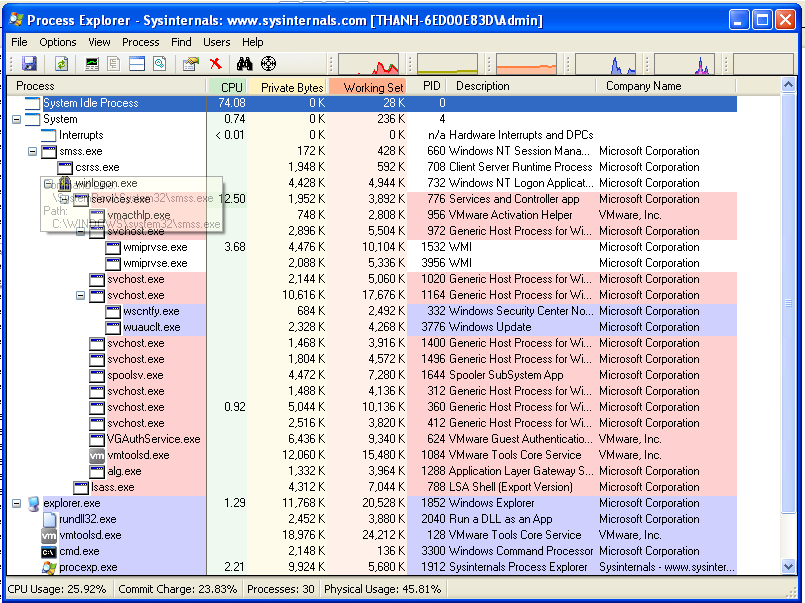
***Making Process Monitor Filter by Process Name***



***Running Process Monitor After Running Malware***



***Running Process Explorer After Running Malware***

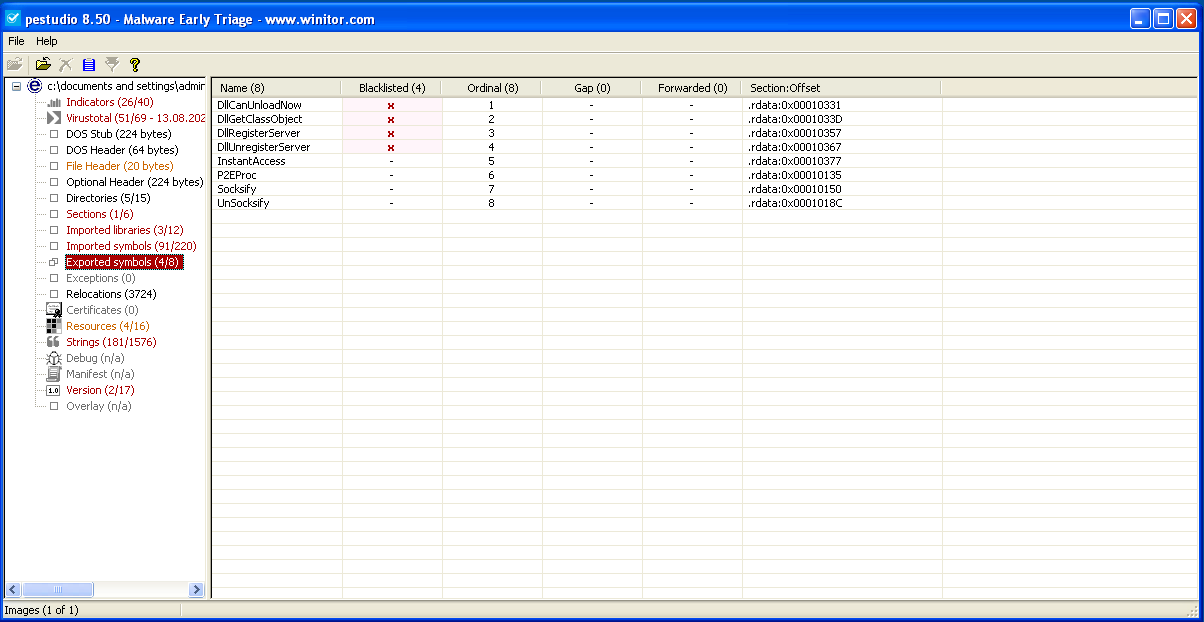


***Downloading Malicious Dll***





***Opening Malicious Dll By Pestudio***



As you can see there are several dll function names and ordinal numbers in Exported symbols.

***Running Malicious Dll***

