

**HARARE INSTITUTE OF TECHNOLOGY**

**INFORMATION SECURITY AND ASSURANCE PART 4**

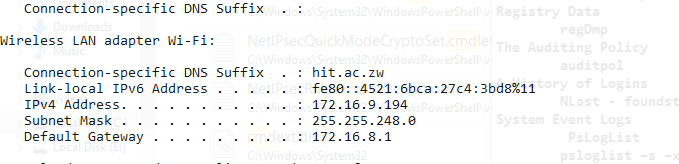
**MICHAEL TKK MHLANGA H140171A**

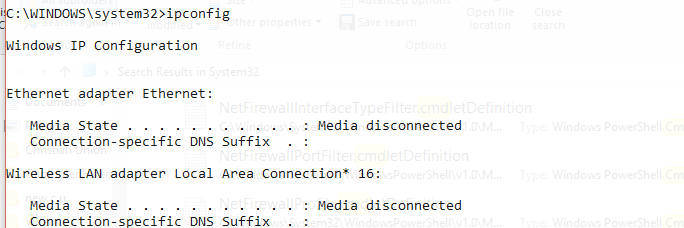
**COMPUTER FORENSICS LAB2 NON VOLATILE DATA**

**TUTOR: MR MARENGEREKE**

**TASK 1:**

**Checking for IP Address and configurations**

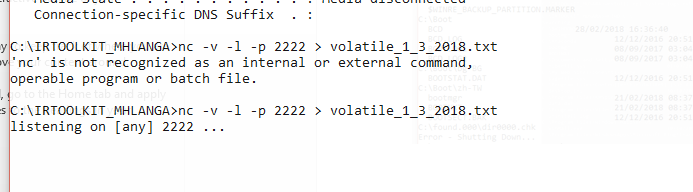




**TASK 2:**

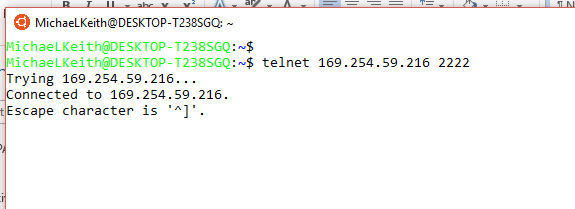
**netcat**

**Starting serve netcat: nc –v –l –p 2222 > volatile\_01\_3\_2018.txt**



**TASK 3:**

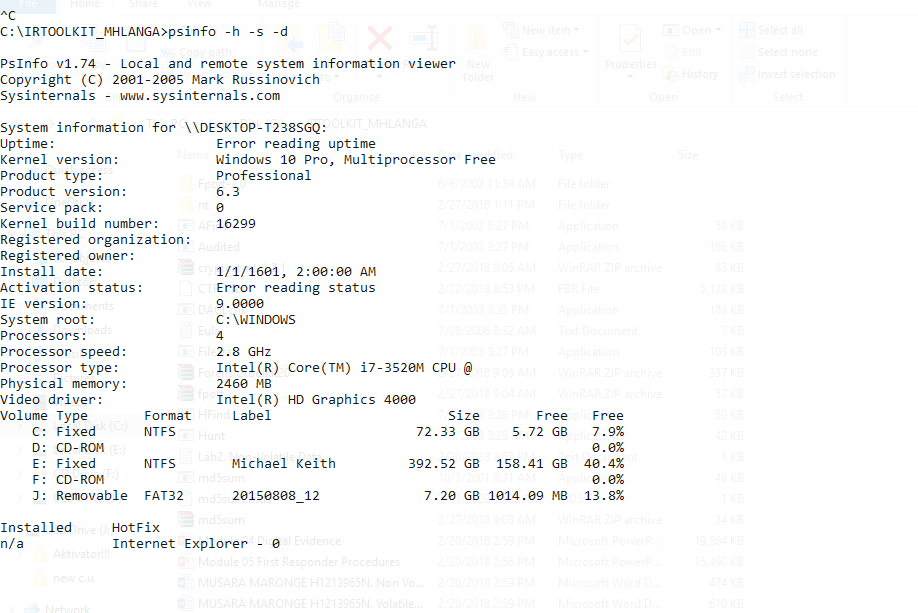
**telnet 169.254.59.216 2222**



**TASK 4:**

**System Version and Patch Level**

**psinfo -h -s –d**

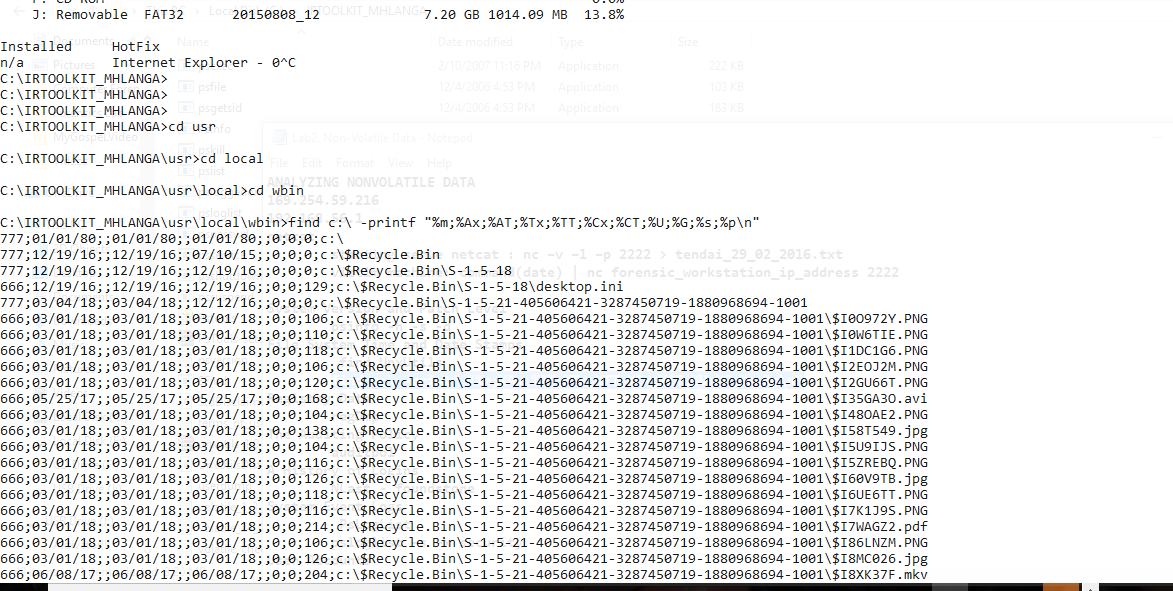


**TASK 5:**

**File System Time and Date Stamps**

**find UnxUtils**

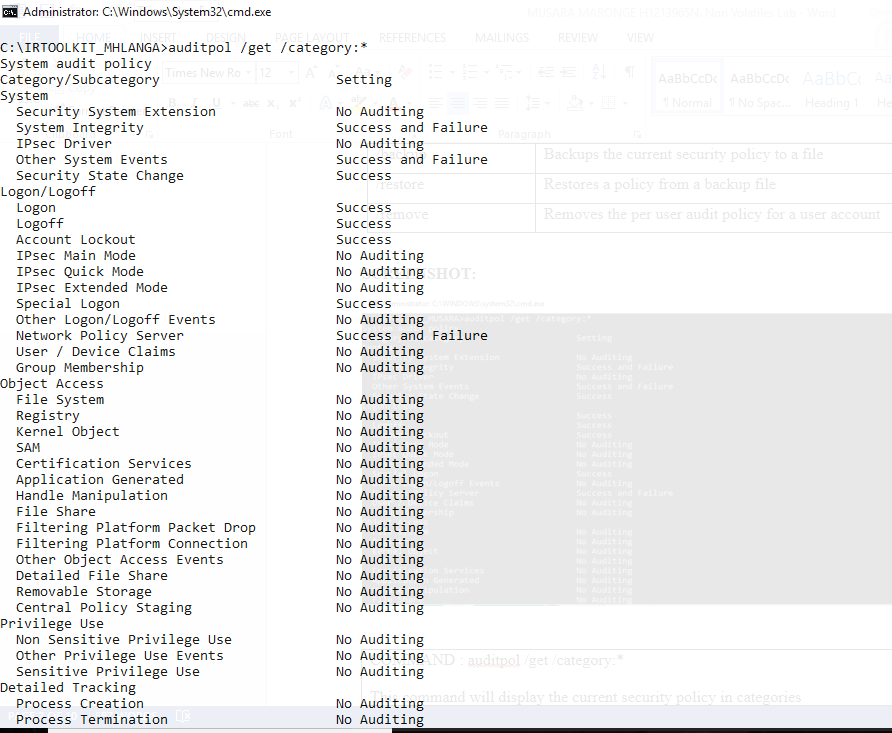
**find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n”**



**TASK 6:**

**The Auditing Policy**

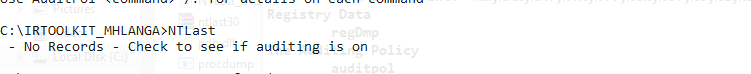
**auditpol**



**TASK 7:**

**A History of Logins**

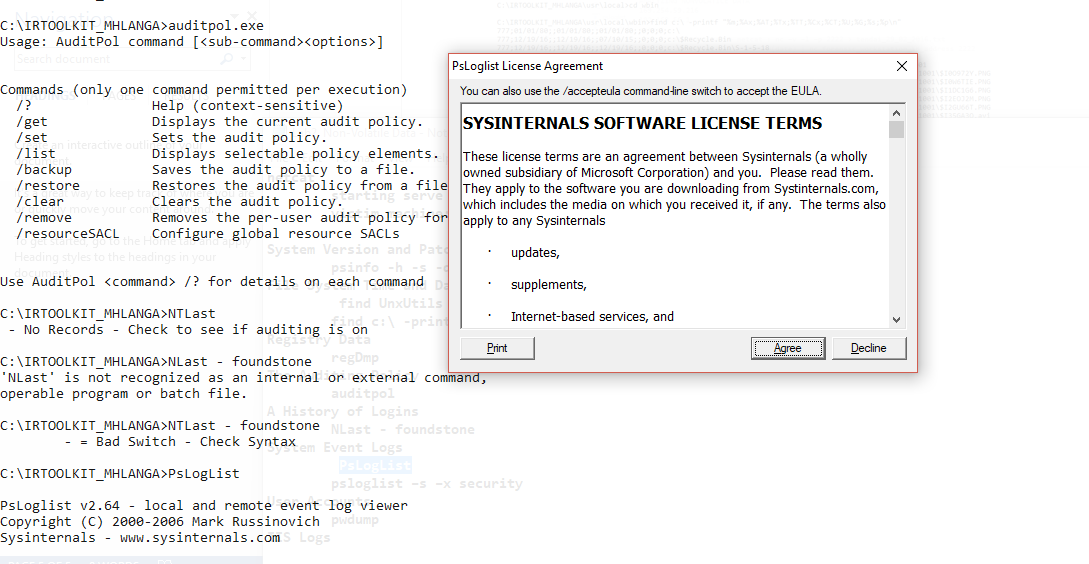
**NTLast**



**TASK 8:**

**System Event Logs**

**PsLogList**



**TASK 9:**

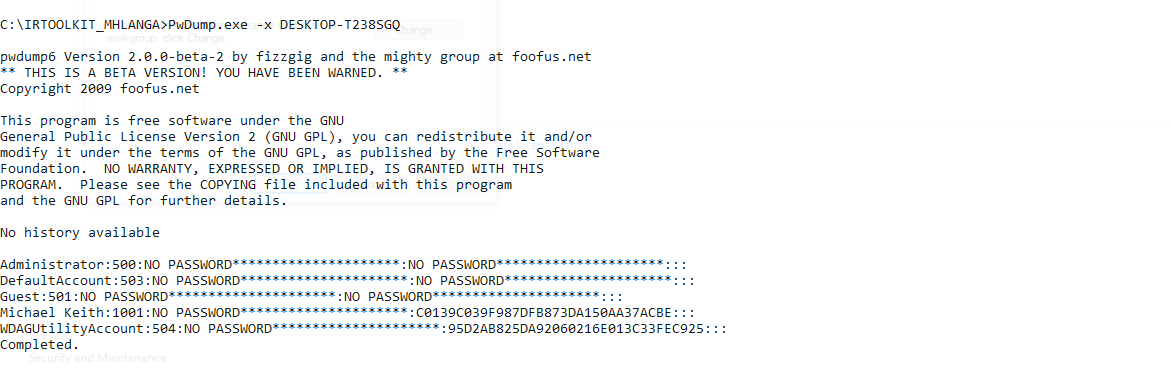
**psloglist –s –x security**



**TASK 10:**

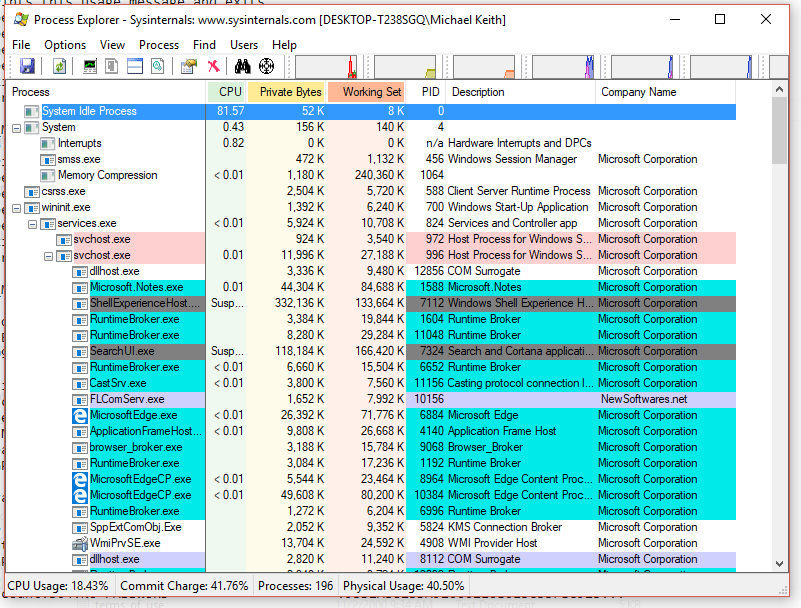
**User Accounts**

**Pwdump**



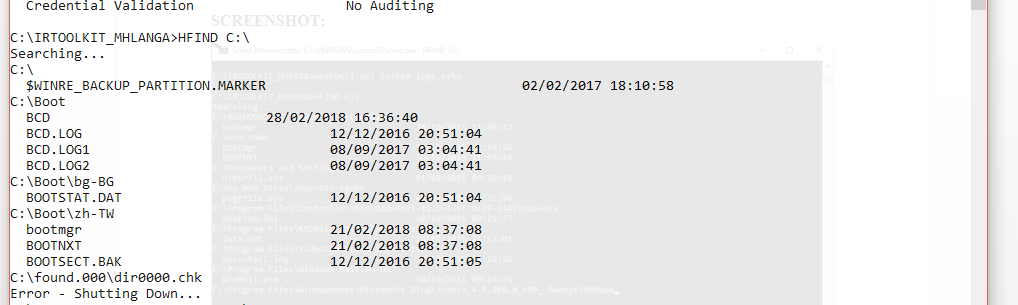
**TASK 11:**

**Suspicious Files**



**TASK 12:**

**Show hidden files**



**TASK 13:**

**Registry Data**

**regDmp**



**TASK 14:**

**IIS Logs**



