

***COMPUTER FORENSICS LAB ONE***

***Windows Live Response***

Assignment by

**NATHAN ISHEANESU NYABVURE**

**H140177Q**

**BACHELOR OF TECHNOLOGY IN INFORMATION SECURITY AND ASSURANCE**

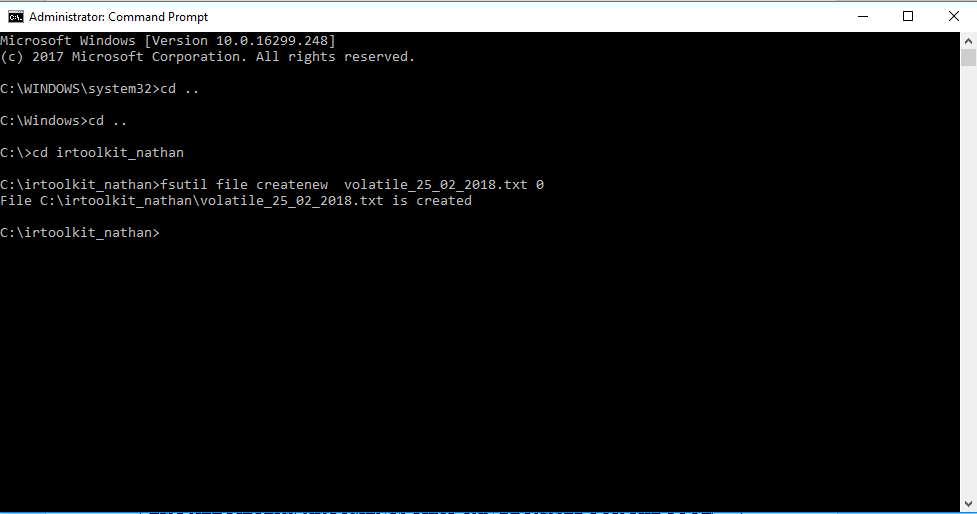
SCHOOLOF INFORMATION SCIENCES AND TECHNOLOGY

**HARARE INSTITUTE OF TECHNOLOGY**

**Lecturer: Mr T Marengereke**

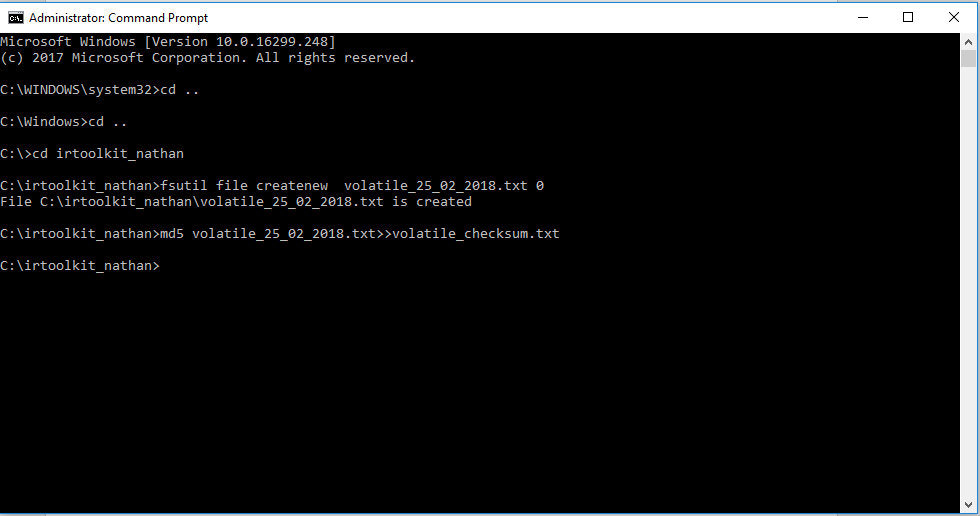
***February 2018***

|  |  |  |
| --- | --- | --- |
| Task 1 Creating a file volatile\_25\_02\_2018.txt | | |
| TOOLS REQUIRED TO PERFORM TASK : cmd.exe | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | | |
| NO ARGUMENTS FOUND |  | |
| filename | | Name of the file to be created |
| length | | Size of the file to be created |



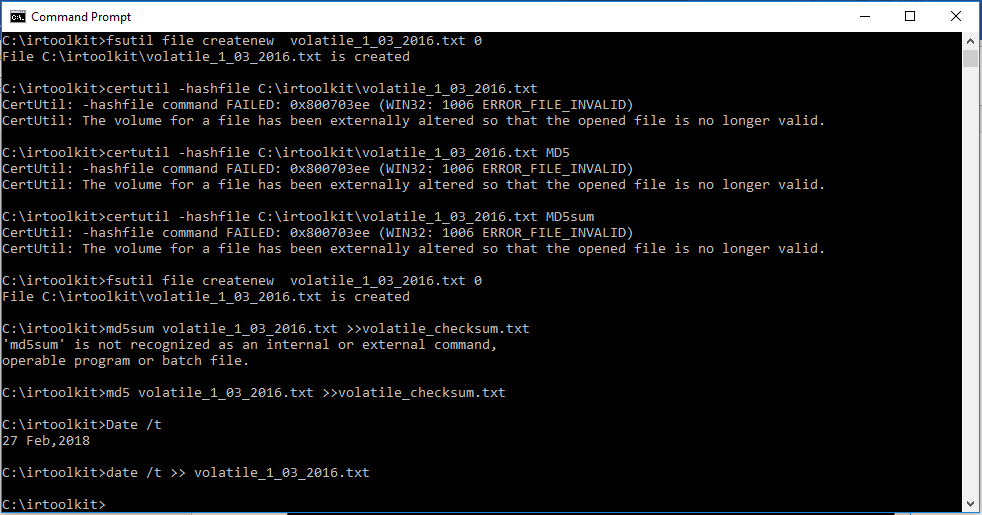
|  |
| --- |
| COMMAND: fsutil file createnew volatile\_25\_02\_2018.txt 0  It will create an empty file named volatile\_25\_02\_2018.txt 0 |

|  |  |
| --- | --- |
| Task 2 Find the md5 of the text file volatile\_25\_02\_2018.txt | |
| TOOLS REQUIRED TO PERFORM TASK : md5sum | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -b | Read the file in binary mode |
| -c | Check md5sums against a given list |
| --status | Don’t output anything, status code shows success |
| -w | Warn about improperly formatted md5sum checksum files |
| --help | Displays help text |
| --version | Output the version information and exit |

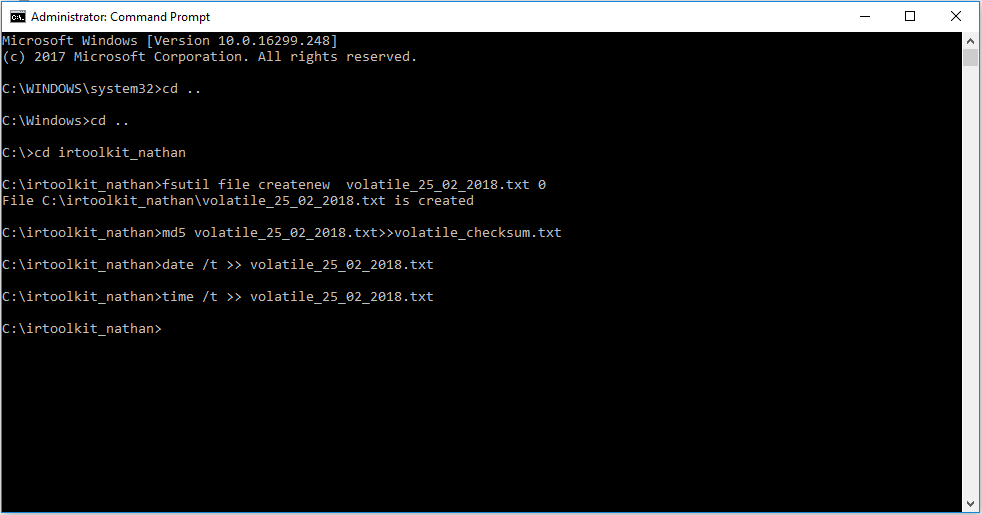


|  |
| --- |
| COMMAND: md5 volatile\_25\_02\_2018.txt>>volatile\_checksum.txt  Creates an md5 of the file volatile\_25\_02\_2018.txt and stores it in the file volatile\_checksum.txt |

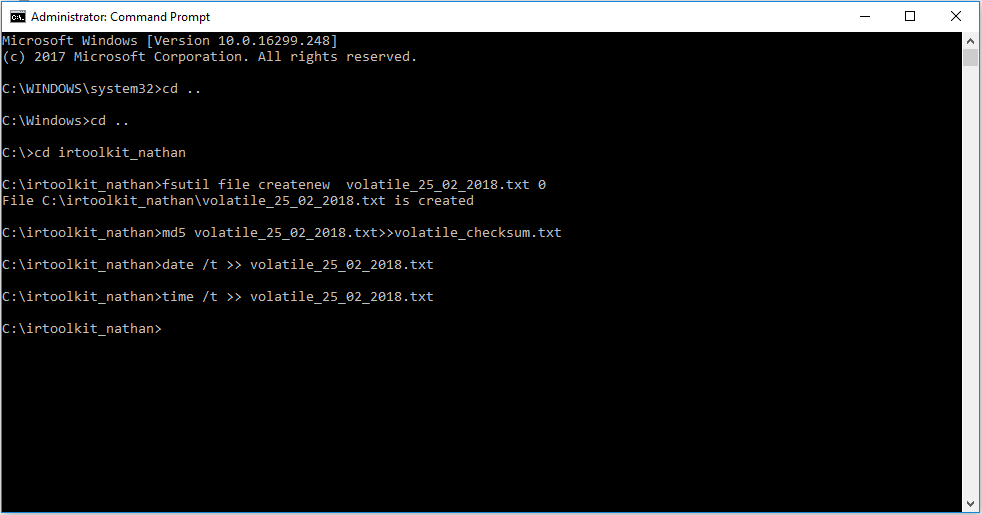
|  |  |
| --- | --- |
| Task 3: Find the system date | |
| TOOLS REQUIRED TO PERFORM TASK : date.exe | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| /t | switch which tells the command to just output the current date, without prompting for a new date. | |



|  |
| --- |
| COMMAND: date /t >> volatile\_1\_0\_2016.txt  Gets the system date and stores it in the text file volatile\_1\_03\_2016.txt |

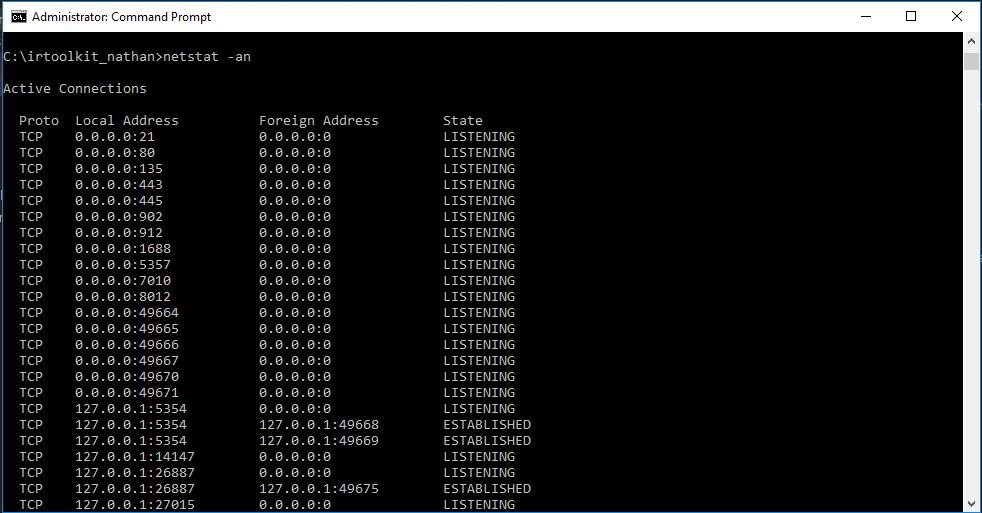


|  |  |
| --- | --- |
| Task 4: Find the system time | |
| TOOLS REQUIRED TO PERFORM TASK : date.exe | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| /t | switch which tells the command to just output the current date, without prompting for a new time. |



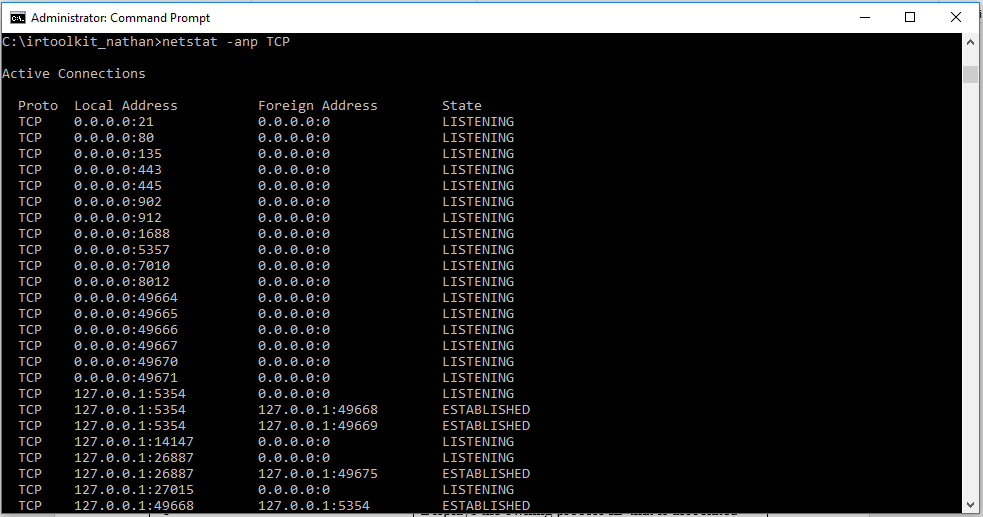
|  |
| --- |
| COMMAND: time /t >> volatile\_1\_03\_2016.txt  Gets the system time and stores it in the text file volatile\_1\_03\_2016.txt |

|  |  |  |
| --- | --- | --- |
| Task 5: Find current network connections | | |
| TOOLS REQUIRED TO PERFORM TASK: netstat | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -a | Displays all connections and listening ports |
| -b | Displays the executable involved in creating each connection or listening port |
| -e | Displays Ethernet statistics |
| -f | Displays the **Fully Qualified Domain Name** for foreign addresses |
| -n | Displays addresses and port numbers in numerical form |
| -o | Displays the owning process ID that is associated with each connection |
| -p proto | Shows the connections for the protocols specified by proto |
| -q | Displays all connections listening ports and bound all non-listening ports. |
| -r | Displays the non-listening ports |
| -s | Displays per protocol statistics |
| -t | Displays current connection offload state |
| -x | Displays network direct connections, listeners and shared endpoints |
| -y | Displays the TCP connection template for all the connections. |
| -interval | Displays selected statistics, pausing interval seconds between each display. |



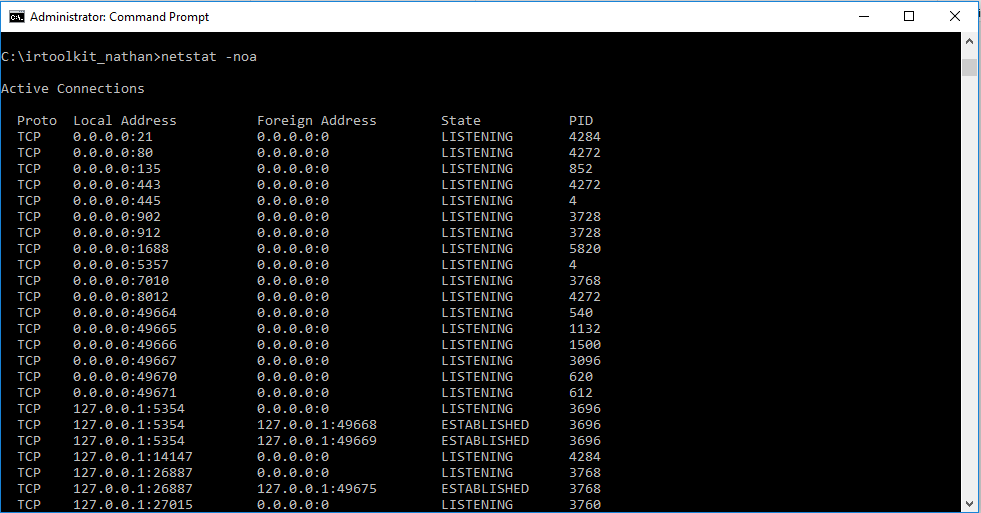
|  |
| --- |
| COMMAND: netsat –an Displays all the connections and listening ports |

|  |  |  |
| --- | --- | --- |
| Task 6: Determining open TCP connections | | |
| TOOLS USED TO PERFORM TASK: netstat –anp tcp | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | | |
| -a | Displays all connections and listening ports |
| -b | Displays the executable involved in creating each connection or listening port |
| -e | Displays Ethernet statistics |
| -f | Displays the Fully Qualified Domain Name for foreign addresses |
| -n | Displays addresses and port numbers in numerical form |
| -o | Displays the owning process ID that is associated with each connection |
| -p proto | Shows the connections for the protocols specified by proto. |
| -q | Displays all connections listening ports and bound all non-listening ports. |
| -r | Displays the non-listening ports |
| -s | Displays per protocol statistics |
| -t | Displays current connection offload state |
| -x | Displays network direct connections, listeners and shared endpoints |
| -y | Displays the TCP connection template for all the connections |
| -interval | Displays selected statistics, pausing interval seconds between each display. |



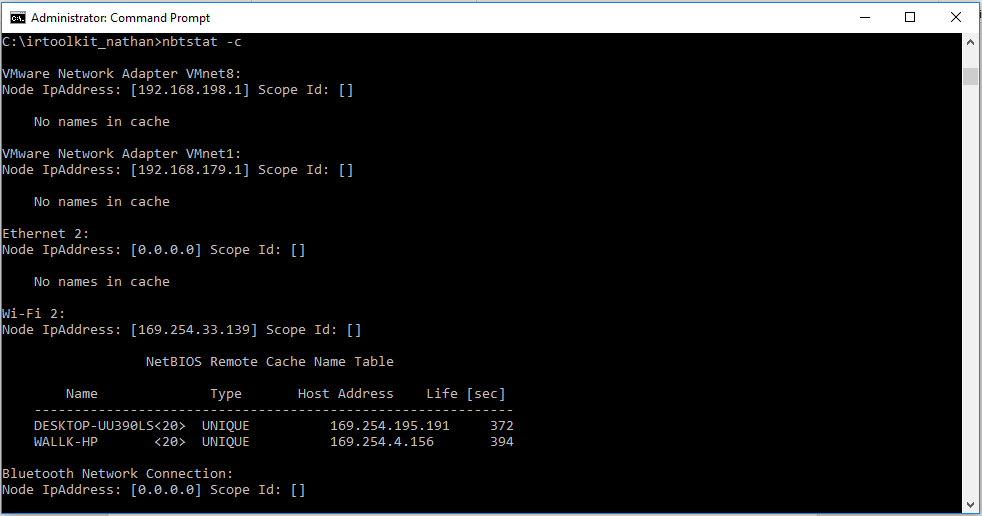
|  |
| --- |
| COMMAND: netsat –anp TCP Displays open TCP ports |

|  |  |  |
| --- | --- | --- |
| Task 7: Determining which executable are opening TCP or UDP Ports | | |
| TOOLS REQUIRED TO PERFORM TASK: netstat | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -a | Displays all connections and listening ports |
| -b | Displays the executable involved in creating each connection or listening port |
| -e | Displays Ethernet statistics |
| -f | Displays the **Fully Qualified Domain Name** for foreign addresses |
| -n | Displays addresses and port numbers in numerical form |
| -o | Displays the owning process ID that is associated with each connection |
| -p proto | Shows the connections for the protocols specified by proto. |
| -q | Displays all connections listening ports and bound all non-listening ports. |
| -r | Displays the non-listening ports |
| -s | Displays per protocol statistics |
| -t | Displays current connection offload state |
| -x | Displays network direct connections, listeners and shared endpoints |
| -y | Displays the TCP connection template for all the connections. |
| -interval | Displays selected statistics, pausing interval seconds between each display. |



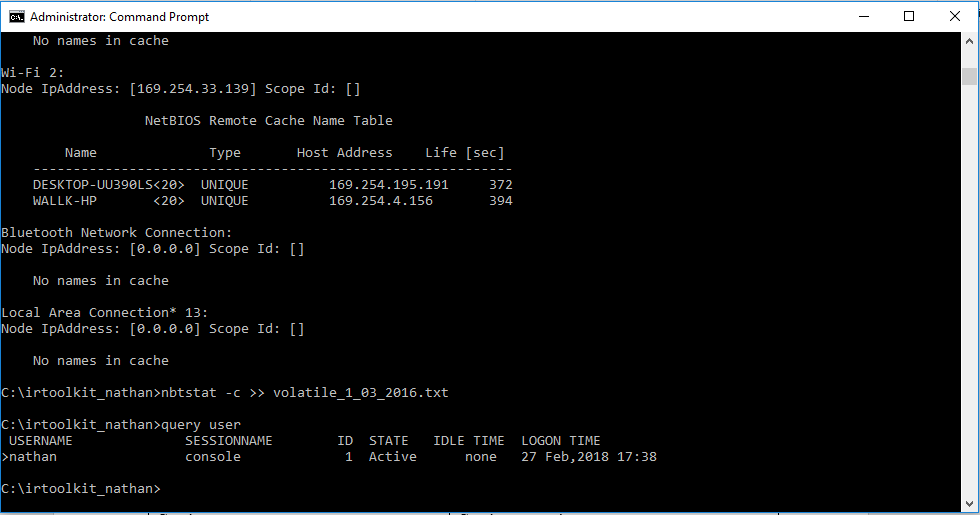
|  |
| --- |
| COMMAND: netsat –noa Displays all executable which are opening TCP or UDP Ports |

|  |  |
| --- | --- |
| Task 8: Find the system cache Netbios NT | |
| TOOLS REQUIRED TO PERFORM TASK : nbtstat | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -c | switch which tells the command to just output the the cache bios NT. |



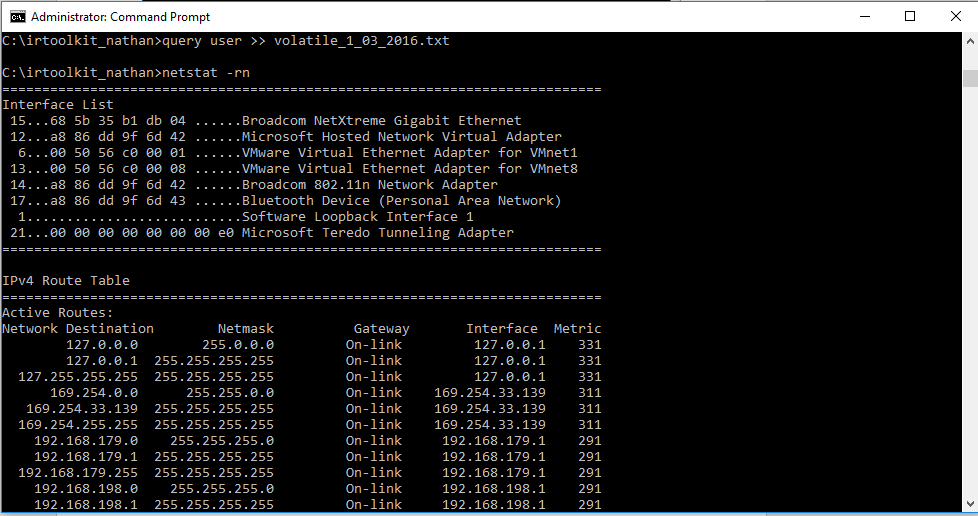
|  |
| --- |
| COMMAND: nbtstat -c |

|  |  |
| --- | --- |
| Task 9: Find the Users Currently Logged On the system | |
| TOOLS REQUIRED TO PERFORM TASK: query user | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| Query user | It provides the username, session name, state and the logged-on time. |



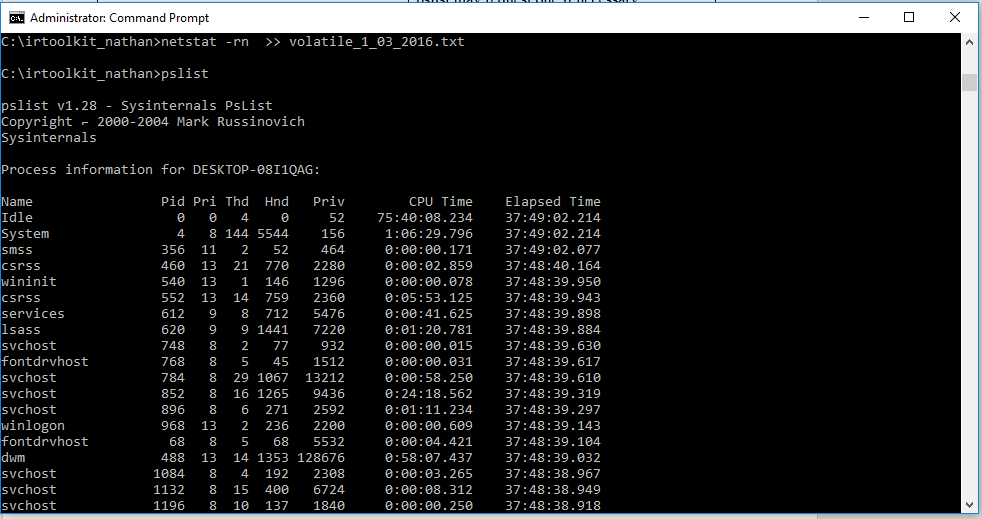
|  |
| --- |
| COMMAND: query user |

|  |  |  |
| --- | --- | --- |
| Task 10: Find the Internal Routing Table | | |
| TOOLS USED TO PERFORM TASK: netstat -rn | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | | |
| -a | Displays all connections and listening ports |
| -b | Displays the executable involved in creating each connection or listening port |
| -e | Displays Ethernet statistics |
| -f | Displays the **Fully Qualified Domain Name** for foreign addresses |
| -n | Displays addresses and port numbers in numerical form |
| -o | Displays the owning process ID that is associated with each connection |
| -p proto | Shows the connections for the protocols specified by proto. |
| -q | Displays all connections listening ports and bound all non-listening ports. |
| -r | Displays the non-listening ports |
| -s | Displays per protocol statistics |
| -t | Displays current connection offload state |
| -x | Displays network direct connections, listeners and shared endpoints |
| -y | Displays the TCP connection template for all the connections. |
| -interval | Displays selected statistics, pausing interval seconds between each display. |



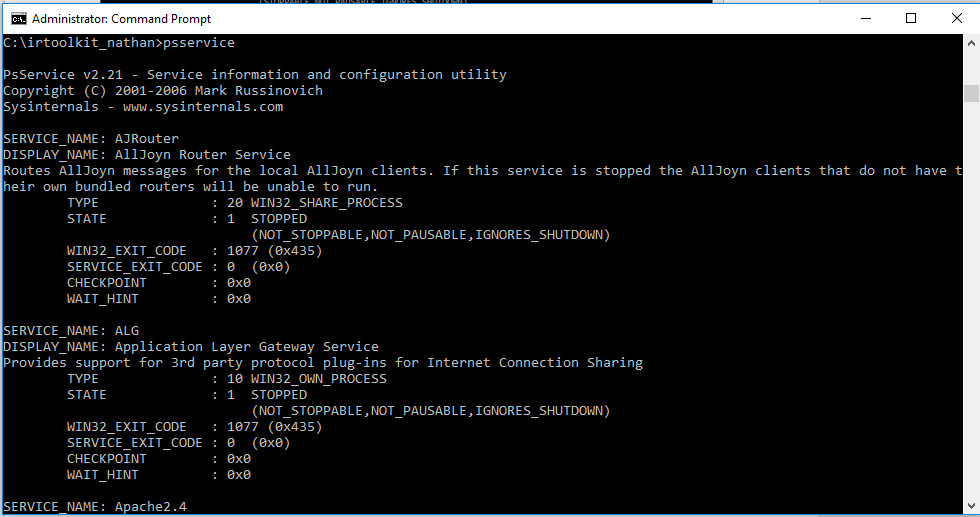
|  |
| --- |
| Command used: netstat –rn. Displays the internal routing table |

|  |  |
| --- | --- |
| Task 11: Running Processes | |
| TOOLS USED TO PERFORM TASK: pslist | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -d | Show thread detail |
| -m | Show memory detail |
| -x | Show process, memory information and threads |
| -t | Show process tree |
| -s [n] | Run in task manager for the optional seconds specified |
| -r n | Task Manager refresh rate in seconds |
| \\computer | Specifies remote computer |
| -u | Optional username for remote login |
| -p | Optional password for remote login. if you don’t request for it on the command line pslist may request one if necessary |
| -name | Show information about the process that begin with the name specified |
| -e | Exact name process zone |
| pid | Show information about the specified system |



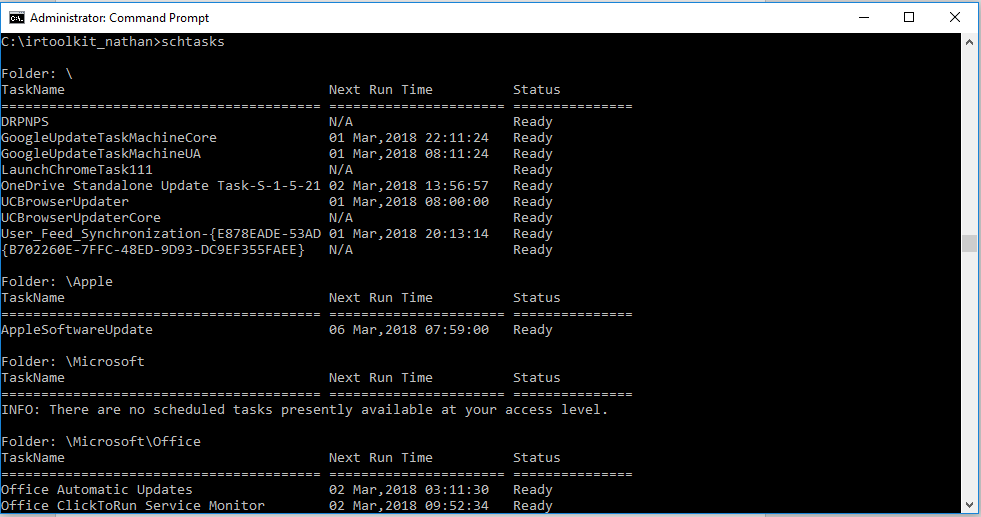
|  |
| --- |
| Command used: pslist. It lists the current processes running. |

|  |  |
| --- | --- |
| Task 12: Running Services | |
| TOOLS TO PERFORM TASK: psservice | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| Query | Queries the status of a service |
| Config | Queries the configuration |
| Setconfig | Sets a configuration |
| Start | Starts a service |
| Stop | Stops a service |
| Restart | Stops and restarts a service |
| Pause | Pause a service |
| Continue | Continue a service |
| Depend | Enumerates the services that depend on the one specified |
| find | Searches for an instance of a service on the network |
| security | Reports the security permissions assigned to a service |



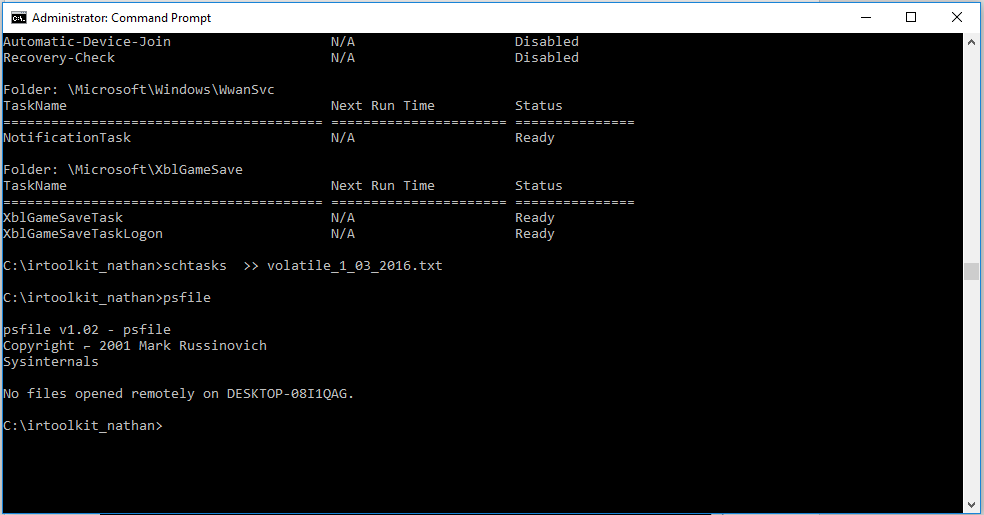
|  |
| --- |
| Command Used :psservice. It gives the list of services that are currently running |

|  |  |
| --- | --- |
| Task 13: Find Scheduled Jobs | |
| TOOLS USED TO PERFOM TASK: schtasks.exe | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| ***NO OPTIOAL ARGUMENTS FOUND*** | |
| /Create | Creates a new scheduled task. |
| /Delete | Deletes the scheduled task(s). |
| /ShowSid | Shows the security identifier corresponding to a scheduled task name. |
| /End | Stops the currently running scheduled task. |
| /Run | Runs the scheduled task on demand. |
| /Change | Changes the properties of scheduled task |
| /Query | Displays all scheduled tasks. |



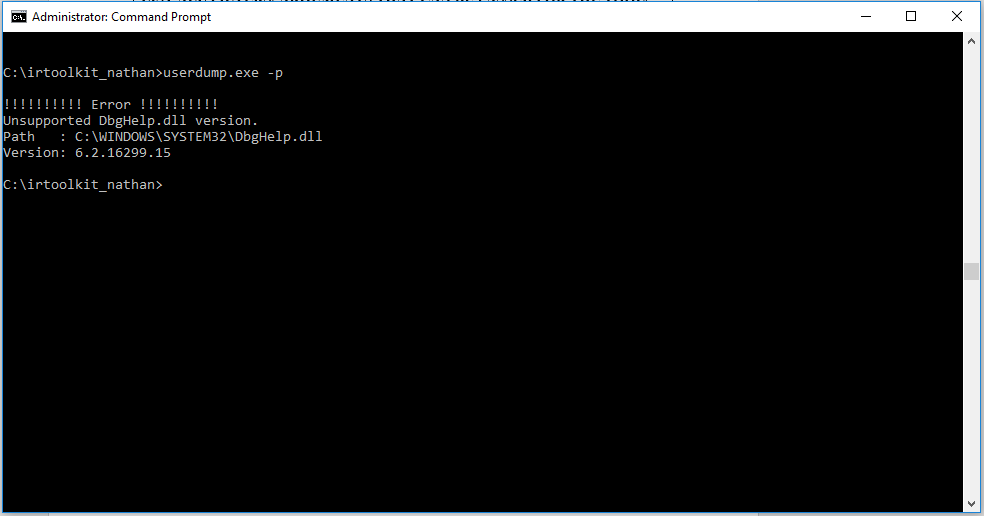
|  |
| --- |
| Command used: schtasks.  It gives the list of tasks that are scheduled to run |

|  |  |
| --- | --- |
| Task 14: find a list of all open files | |
| ***TOOLS TO PERFORM TASK: psfile*** | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -u | Specifies optional user name for login to  remote computer |
| -p | Specifies password for user name. |
| Id | Id of file to print information for or close |
| Path | Full or partial path of files to match. |
| -c | Closes file identified by file Id. |



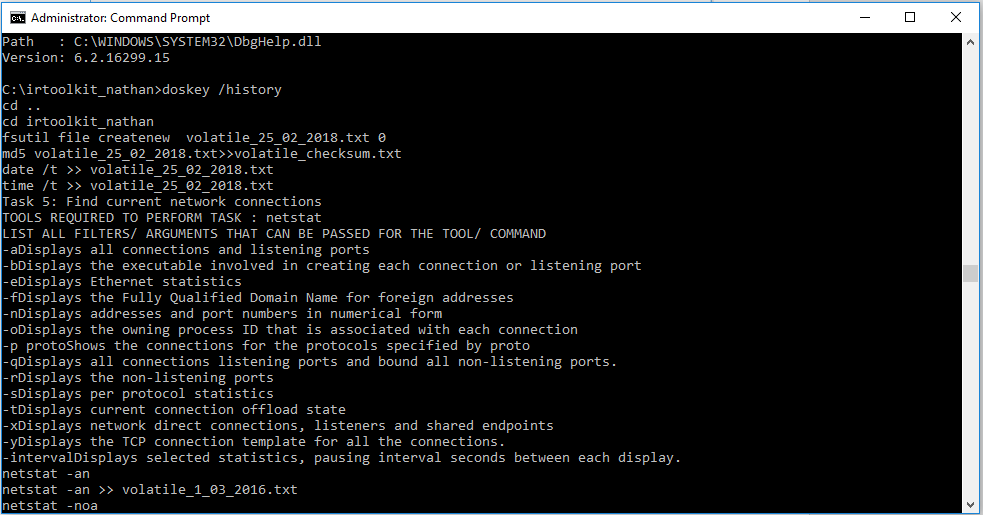
|  |
| --- |
| Command Used: psfile. It gives the list of remotely opened files |

|  |  |  |
| --- | --- | --- |
| Task 15: Process Image Dumps | | |
| TOOLS TO BE USED: userdump | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | | |
| -p | Displays a list of running process and process Id’s |
| -k | Optionally causes a process to be killed after being dumped |
| -m | Same as above, except that it dumps multiple files |
| -d | Specifies the directory to dump the files |
| -g | Same as above, except that it dumps win32 gui apps that appear to hang |



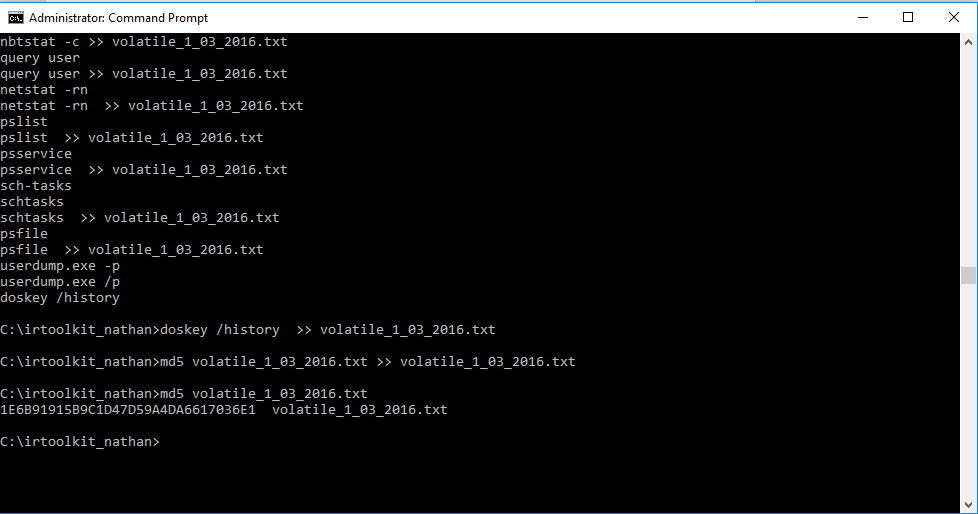
|  |
| --- |
| Command Used:userdump /p. was not successful in displaying a list of running processes and process ID’s |

|  |
| --- |
| Task16: Find the History of all commands Executed |
| TOOLS TO BE USED: cmd.exe | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL COMMAND*** | |
| ***NO OPTIONAL ARGUMENTS FOUND*** | |



|  |
| --- |
| Command Used: DOSKEY /history. Lists the history of all the commands performed |

|  |  |
| --- | --- |
| Task17: Calculate the second md5 of volatile\_1\_03\_2016.txt | |
| TOOLS REQUIRED TO PERFORM TASK: md5sum | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | |
| -b | Read the file in binary mode |
| -c | Check md5sums against a given list |
| --status | Don’t output anything, status code shows success |
| -w | Warn about improperly formatted md5sum checksum files |
| --help | Displays help text |
| --version | Output the version information and exit |



|  |
| --- |
| COMMAND: md5 volatile\_1\_03\_2016.txt >> volatile\_1\_03\_2016.txt  Creates an md5 of the file volatile\_1\_03\_2016.txt and stores it in the file in the file volatile\_1\_03\_2016.txt |