Windows Artifacts

1. Learn to run the command line tool as administrator to collect some of these volatile and non-volatile information.

* Open the command line window as an administrator
* Figure out how to execute the following commands using the internet and the tool help.
  + doskey /history
  + time/t
  + net use
  + net sessions
  + net file
  + openfiles
  + nbtstat –c
  + netstat
  + tasklist
  + ipconfig
* For each command, explain the forensic use of the output, identify the exact command and any options used and include the text file output of the command.

1. Research tools that can strip metadata. List 3 and explain if they are open source or closed source and any other interesting information about them.
2. Work with FTK Imager to become very familiar with the tool.