# Exercise 5

## 07/09/2021

## The Windows Command Line

Forensics investigators should be familiar with the use of the Windows command line when they investigate computers that use the Windows operating system. Forensics software sometimes necessitates the use of the command line. Forensics recovery and data reconstruction requires an understanding of the command line syntax. Before shutting down a computer, the forensic examiner should often capture the volatile information in the system's RAM. Information such as current IP address, contents of RAM, Address Resolution Protocol (ARP) tables and current network connection status are not available once the computer has been turned off. Hence the forensic examiner must be familiar with the commands and techniques used to obtain such information on site.

Some DOS commands. Try these.

CD MD RD COPY ATTRIB DISKCOPY DATE TIME DIR PAUSE NETSTAT TYPE DEL VER DOSKEY PATH PROMPT LABEL VOL DEFRAG XCOPY ECHO REM MOVE EXIT FORMAT REN TREE MORE PRINT HELP IPCONFIG ARP CMD CALL CHCP CHKDSK CHOICE CLS ERASE DIR FC COMP FIND FOR IF MODE RECOVER SET SORT SUBST

Note: Some of the above commands are internal commands. Others are external commands. An external command is an MS-DOS command that is not included in command.com. External commands are commonly external either because they have large requirements or are not commonly used commands. Some external commands are in the above list. Some more are listed here:

BOOTSECT BCTEDIT DISKCOMP HOSTNAME ICACLS CHKNTFS NBTSTAT NET NETSH PING NSLOOKUP ROUTE PATHPING SYSTEMINFO WMIC FTP TRACERT

See https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands

Exercise

1) Use commands to find the IPv4 address and subnet mask of your computer.

2) Create a batch file that will capture the following volatile information from an evidence system and store it a file.

Current IPv4 address

Current date

Current time

ARP table

Network connection information

Take screenshots in both cases and include them in your submission.

Note: The ARP (Address Resolution Protocol) cache is a collection of ARP entries (mostly dynamic) that are created when a hostname is resolved to an IP address and then an IP address is resolved to a MAC address (so the computer can effectively communicate with the IP address). ARP cache has the disadvantage of being used by hackers and cyber attackers. ARP cache helps the attackers hide behind a fake IP address and do the harm without being caught. ARP cache can also help to prevent the attacks.

(see https://en.wikipedia.org/wiki/ARP_cache)