Matthias Smet
Studentnumber: 23214388

1. Tools

The following tools where used on a windows computer and work on a 64 bit version of windows 10 and 11. (CLI only)

Nr.	Tool name	Motivation for order
1	[1]powercfg	Preventing the system from entering sleep mode or activating the screensaver is essential to ensure uninterrupted data collection.
2	[2]Regedit	Preventing the system from entering sleep mode or activating the screensaver is essential to ensure uninterrupted data collection.
2	[3]manage-bde	Checking BitLocker status early is important in a forensic context as it identifies encrypted drives. Knowing this upfront can be critical for the subsequent data collection process.
3	[4]hostname	The hostname command retrieves the name of the local host or computer. This information is essential for identifying the specific machine being analyzed, especially in environments with multiple computers. It helps in correlating collected data with the correct system in forensic investigations.
4	[5]systeminfo	The systeminfo command gathers comprehensive information about the operating system, including its name and version. This data is important to understand the operating environment, as different OS versions can have different features, vulnerabilities, and logging capabilities. It's also vital for ensuring compatibility with forensic tools and interpreting collected data accurately.
5	[6]DumpIt.exe	Capturing the memory dump early is crucial as it provides a snapshot of the system's state at the beginning of the forensic process. Memory contains valuable information that can change rapidly.

[1] https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/powercfg-command-line-options
[2] https://answers.microsoft.com/en-us/windows/forum/all/how-do-i-turn-off-screen-saver-momentarily/4ae993a8-bd51-4344-a3fd-0caeb8a5cf09
[3] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/manage-bde
[4] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/hostname
[5] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo
[6] https://www.magnetforensics.com/blog/magnet-dumpit-for-windows-magnet-dumpit-for-linux-now-available/

6	[7]tasklist	Identifying running virtual machines and encryption processes can be crucial, as they might hold significant forensic data or indicate system usage patterns.
7	[8]netstat	The netstat command provides details about all active network connections and listening ports, along with the associated process IDs. In forensic analysis, this information is invaluable for identifying unauthorized network connections, potential data exfiltration points, or signs of remote access tools. Since network connections can change rapidly, capturing this information early is important.
8	[9]arp	The ARP (Address Resolution Protocol) table contains details about the IP to physical address (MAC address) mapping on the local network. This information can help in identifying other devices the system was communicating with on the local network, which is useful in investigations involving network activity and lateral movement.
9	[10]ipconfig	Running ipconfig provides comprehensive details about the system's network configuration, including IP addresses, subnet masks, default gateways, and DNS servers. This data is fundamental to understanding the network context of the system, such as how it's connected to the network, its role in the network, and potential communication paths.
10	[11]net session	This step is important to understand active user connections to the machine, which can be critical in understanding how the system was being accessed.
11	[12]robocopy	Executed towards the end as it's a less volatile data collection. This step is potentially time-consuming and is placed later to ensure more volatile data is captured first.

[7] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist
[8] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
[9] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/arp
[10] https://www.med.unc.edu/it/guide/operating-systems/how-do-i-find-the-host-name-ip-address-or-physical-address-of-my-machine/
[11] https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh750729(v=ws.11)
[12] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/robocopy

2. Suspect Picture Files

Command Used: robocopy *.jpg *.png /S /COPYALL /DCOPY:T /MIN:10000 /XD "Windows" "Program Files" "Program Files (x86)" "ProgramData"

File Types Targeted: The script is set to look for .jpg and .png files, which are common image file formats.

Source and Destination Directories:

- The script iterates over all potential drive letters from C to Z. The script checks each drive letter to ensure no location is missed.
- For each drive, robocopy is used to search for and copy the specified file types.
- The destination for these files is set to the Pictures folder within the “ForensicFolder” on the USB drive.

Copying Options:

- **/S**: Copies subdirectories (but not empty ones).
- **/COPYALL**: Copies all file attributes, including hidden and system attributes.
- **/DCOPY:T**: Copies directory timestamps.
- **/MIN:10000**: Excludes very small files (under 10,000 bytes) to avoid copying thumbnails.
- **/XD**: Excludes certain system directories from the copying process to speed the process.

Execution Considerations:

- The script checks each drive letter to ensure no location is missed.
- This step can take some time, especially if there are many images or large drives.

3. Image Dump

Command Used:"%USBDrive%\Tools\DumpIt.exe" /O "%MemoryDump%\MemoryDump.raw"

Execution of Memory Dump:

The command "%USBDrive%\Tools\DumpIt.exe" /O "%MemoryDump%\MemoryDump.raw" is used to execute DumpIt.

%USBDrive%\Tools\DumpIt.exe specifies the location of the DumpIt executable, stored on the USB drive.

/O "%MemoryDump%\MemoryDump.raw" directs DumpIt to output the memory dump into a file named MemoryDump.raw located in the MemoryDump directory on the USB drive.

4. Other Volatile Information

Collect Information about Running Processes

tasklist

Process: Generates a list of all processes running on the system.

Significance: Vital for identifying active applications and services, including any malicious processes.

Collect Information about Active Network Connections

netstat -ano

- **Process**: This command provides a detailed view of all active network connections and listening ports, along with the associated process IDs (the -ano flags).

Collect ARP table

arp -a

- **Process**: The arp -a command displays the ARP (Address Resolution Protocol) table, which maps IP addresses to their corresponding physical MAC (Media Access Control) addresses on the local network.

Collect IP Configuration

ipconfig /all

- **Process**: This command outputs the full network configuration of the system, including IP addresses for all network interfaces, subnet masks, default gateways, DNS servers, and other network settings.

Collect DNS Cache Information

ipconfig /displaydns > "%DNSCacheFile%"

- **Process:** The command ipconfig /displaydns is executed to display the contents of the Domain Name System (DNS) cache.

Check for Running Virtual Machines

tasklist | findstr "vmware-vmx.exe VirtualBoxVM.exe vmwp.exe"

- **Process**: The script searches for processes related to virtual machines and encryption tools.

Collect Active Network Sessions

net session

- **Process**: Lists active network sessions.

5. Batch File

```
@echo off
SETLOCAL ENABLEDELAYEDEXPANSION

[13]:: Determine the drive letter of the USB drive
[14]SET USBDrive=%~d0

:: Set directories on the USB drive
[15]SET ForensicFolder=%USBDrive%\ForensicData
SET BitLockerInfo=%ForensicFolder%\BitLockerInfo.txt
SET SystemInfoFile=%ForensicFolder%\SystemInfo.txt
SET TimeComparison=%ForensicFolder%\TimeComparison.txt
SET MemoryDump=%ForensicFolder%\MemoryDump
SET ProcessList=%ForensicFolder%\ProcessList.txt
SET NetworkConnections=%ForensicFolder%\NetworkConnections.txt
SET ARPTable=%ForensicFolder%\ARPTable.txt
SET IPConfigAll=%ForensicFolder%\IPConfigAll.txt
SET DNSCacheFile=%ForensicFolder%\DNSCache.txt
SET VMInfo=%ForensicFolder%\VMInfo.txt
SET EncryptionProcesses=%ForensicFolder%\EncryptionProcesses.txt
SET ActiveNetworkSessions=%ForensicFolder%\ActiveNetworkSessions.txt
SET PictureFolder=%ForensicFolder%\Pictures

:: Turn off the screensaver and prevent sleep mode
REG ADD "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveActive /t
REG_SZ /d 0 /f
powercfg -change -standby-timeout-ac 0
powercfg -change -standby-timeout-dc 0
powercfg -change -monitor-timeout-ac 0
powercfg -change -monitor-timeout-dc 0
```

[13] https://superuser.com/questions/82231/how-do-i-do-comments-at-a-windows-command-prompt
[14] https://community.spiceworks.com/topic/2263998-running-bat-files-from-cmd-when-drive-letter-changes (user GmCity)
[15] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/set_1

```
:: Check and Create Folders
IF NOT EXIST "%ForensicFolder%" MKDIR "%ForensicFolder%"
IF NOT EXIST "%PictureFolder%" MKDIR "%PictureFolder%"
IF NOT EXIST "%MemoryDump%" MKDIR "%MemoryDump%"

:: Check for BitLocker Encryption and Retrieve Recovery Key for each drive
ECHO Retrieving BitLocker Status and Recovery Keys > "%BitLockerInfo%"
FOR %%D IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
   manage-bde -status %%D: >> "%BitLockerInfo%"
   manage-bde -protectors -get %%D: >> "%BitLockerInfo%"
)

:: Collect System Information (Hostname, User, OS Details)
ECHO Collecting System Information...
ECHO Hostname: > "%SystemInfoFile%"
hostname >> "%SystemInfoFile%"
ECHO. >> "%SystemInfoFile%"
ECHO Current User: >> "%SystemInfoFile%"
echo *%USERNAME% >> "%SystemInfoFile%"
ECHO. >> "%SystemInfoFile%"
ECHO Operating System Details: >> "%SystemInfoFile%"
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" >> "%SystemInfoFile%"
ECHO. >> "%SystemInfoFile%"

:: Acquire Memory Dump with Magnet RAM Capture (DumpIt)
ECHO Acquiring Memory Dump...
"%USBDrive%\Tools\DumpIt.exe" /O "%MemoryDump%\MemoryDump.raw"

:: Collect Information about Running Processes
ECHO Collecting Running Processes...
tasklist > "%ProcessList%"
```

[16] https://stackoverflow.com/questions/4165387/create-folder-with-batch-but-only-if-it-doesnt-already-exist
[17] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/for

```
:: Collect Information about Active Network Connections
ECHO Collecting Active Network Connections...
netstat -ano > "%NetworkConnections%"

:: Collect ARP Table
ECHO Collecting ARP Table...
arp -a > "%ARPTable%"

:: Collect IP Configuration
ECHO Collecting IP Configuration...
ipconfig /all > "%IPConfigAll%"

:: Collect DNS Cache Information
ECHO Collecting DNS Cache Information...
ipconfig /displaydns > "%DNSCacheFile%"

:: Collect Active Network Sessions
ECHO Collecting Active Network Sessions...
net session > "%ActiveNetworkSessions%"

:: Copy Picture Files from each drive (excluding very small files and system directories)
ECHO Copying Picture Files...
FOR %%D IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
    robocopy %%D:\ "%PictureFolder%" *.jpg *.png /S /COPYALL /DCOPY:T /MIN:10000
/XD "Windows" "Program Files" "Program Files (x86)" "ProgramData"
)

ECHO Forensic data collection complete.
```

[18] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/echo
[19] https://lazyadmin.nl/it/how-to-use-ipconfig-displaydns/

6. Results

Executing the script you provided would result in a collection forensic data from a Windows computer. Here's an overview of the results you would get from each part of the script:

- The directory “Pictures” contains all the pictures. (With the subdirectories).
- The directory “MemoryDump” contains the memory dump.