NAME: \_\_Coleton Sanheim\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Lab 3:   
Live Response

ITSC 306: Computer Forensics

Table of Contents

[Lab Outcome 2](#_Toc494185134)

[Readings 2](#_Toc494185135)

[Introduction 2](#_Toc494185136)

[1.0 Creating the Live Response Kit for a Windows 7 System 3](#_Toc494185137)

[2.0 Scripting Your Response 8](#_Toc494185138)

[Scripting Your LRK 8](#_Toc494185139)

[3.0 Running the Script 12](#_Toc494185140)

[References 15](#_Toc494185141)

ITSC 306: Computer Forensics

Lab 3: Live Response

Lab Outcome

* Create a Windows Live Response Kit.

Readings

* Chapter 7, Live Data Collection, in *Incident Response & Computer Forensics*, 3rd ed.
* [Command-line reference A-Z](https://technet.microsoft.com/en-ca/library/bb490890.aspx) (https://technet.microsoft.com/en-ca/library/bb490890.aspx)

Introduction

Sometimes it is necessary to view the contents of a running system before pulling the plug and imaging the hard drive. This is usually done to gather volatile information that will be lost forever once the system loses power. The goal is to gather the required information as quickly as possible while impacting the system as little as possible.

In this lab, you will create a Live Response Kit (LRK) for a Windows 7 system. You will then test the LRK on the system and examine the results of the test.

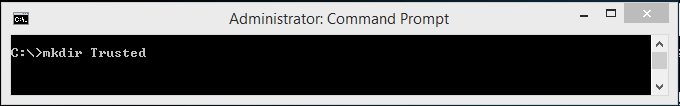
1. Creating the Live Response Kit for a Windows 7 System

It is important to be comfortable running command line tools.

1. Download the following tools:

* [Sysinternals Suite](https://technet.microsoft.com/en-us/sysinternals/bb842062) (https://technet.microsoft.com/en-us/sysinternals/bb842062)
* [Debugging Tools for Windows 10 (WinDbg)](https://developer.microsoft.com/en-us/windows/hardware/download-windbg) (https://developer.microsoft.com/en-us/windows/hardware/download-windbg)
* [OpenPorts](http://www.majorgeeks.com/mg/getmirror/openports,2.html) (http://www.majorgeeks.com/mg/getmirror/openports,2.html)
* [NetCat for Windows](https://github.com/diegocr/netcat) (https://github.com/diegocr/netcat)
* [Md5sum.exe](http://www.etree.org/md5com.html) (http://www.etree.org/md5com.html)

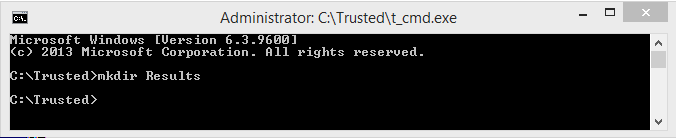
1. Create a directory in the root of the C: drive named **Trusted**.



**Figure 1:**

Used with permission from Microsoft.

1. In this directory, create a folder called **Results** and a folder called **en-US**.
2. Place copies of the files you will use in your LRK in the **Trusted** directory.



**Figure 2:**

Used with permission from Microsoft.

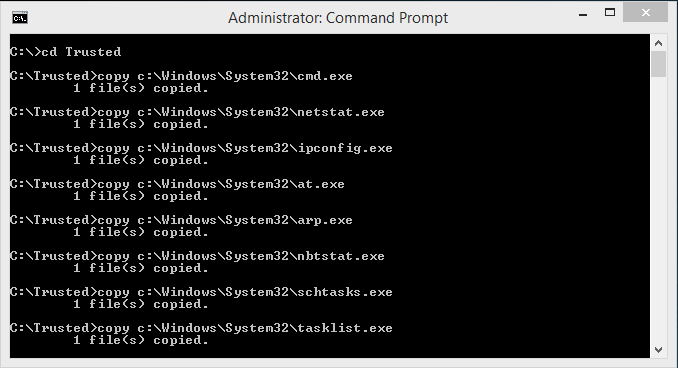
Normally, you would get these files from a recent, clean build of the operating system you intend to examine with this LRK. For this lab, use the system binaries from your local system to save time.

1. Copy the following files to your **Trusted** directory:

* cmd.exe [system32 folder]
* arp.exe [system32 folder]
* at.exe [system32 folder]
* handle64.exe [sysinternals]
* ipconfig.exe [system32 folder]
* logonsessions64.exe [sysinternals]
* md5sum.exe [http://www.etree.org/cgi-bin/counter...are/md5sum.exe]
* nc.exe [https://github.com/diegocr/netcat]
* netstat.exe [system32 folder]
* openports.exe [http://www.majorgeeks.com…/openports,2.html]
* psfile64.exe [sysinternals]
* psinfo64.exe [sysinternals]
* psloggedon64.exe [sysinternals]
* psloglist.exe [sysinternals]
* psservice64.exe [sysinternals]
* schtasks.exe [system32 folder]
* tasklist.exe [system32 folder]
* dumpit.exe [https://www.downloadcrew.com/article/23854-dumpit]
* cygwin1.dll [https://sourceforge.net/projects/cygwin1-dll]
* pslist64.exe [sysinternals]
* cmdext.dll [system32 folder]
* cmdial32.dll [system32 folder]

Graphical user interface, table

Description automatically generated



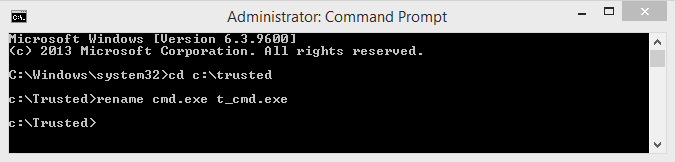
**Figure 3:**

Used with permission from Microsoft.

Ordinarily, you would prepend each file name with **t\_** to know that you are running your trusted tools when the batch file is run and to ensure that you don’t run something from the suspect system.

For the purposes of this lab, however, you *won’t* prepend each file name with **t\_**.

The command to rename a file is illustrated in Figure 4. Another option would be to use File Explorer, go into the Trusted directory, click the file name and then add **t\_** to the beginning of each executable.



**Figure 4:**

Used with permission from Microsoft.

Some of the executables may require DLLs to run. You need to add these DLLs to the Trusted directory. Two applications you can use to determine this PEview (32 bit) and Dependency Walker (32 & 64 bit).

Most executables look for their supporting files in the following search order:

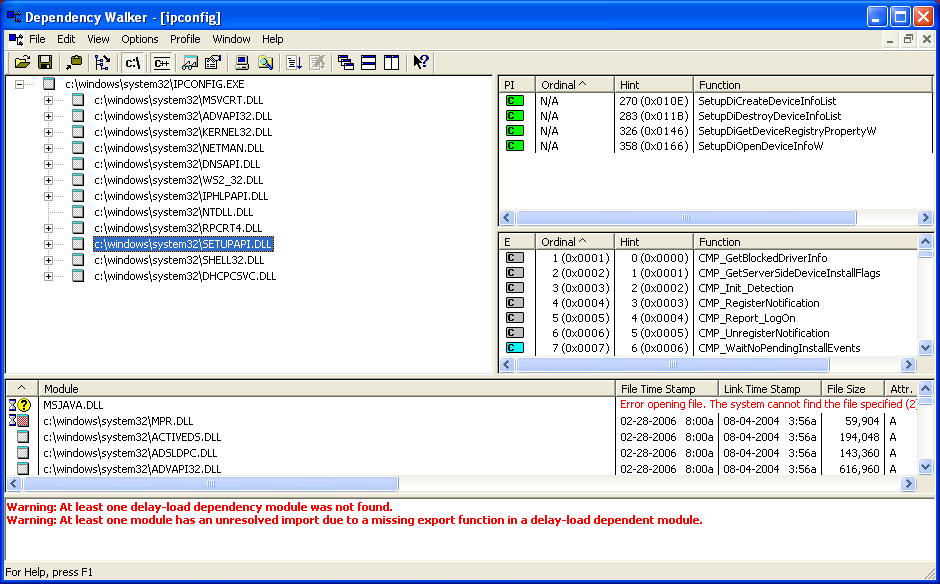
1. The current working directory
2. The directory the program resides in
3. The system32 directory

Some newer Microsoft binaries are hard coded to look in a particular directory path first.

The operating system treats some system DLLs specially. The following registry key contains a list of system DLLs which the system loads ONLY from the system32 directory:

* HKLM\System\CurrentControlSet\ Control\Session\Manager\KnownDLLs

This registry key simply feeds a kernel object called \KnownDLLs on bootup.



**Figure 3:**

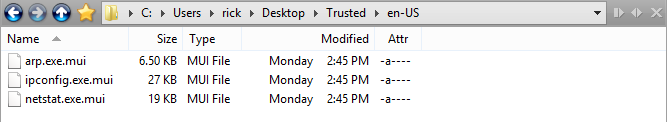
Used with permission from Microsoft.

For example, ipconfig.exe requires numerous DLL files to run properly. In this lab, don’t add the DLLs and let the applications use the DLLs on the suspect system.

1. Copy the following files into the folder **en-US**:

* arp.exe.mui C:\Windows\System32\en-US]
* ipconfig.exe.mui [C:\Windows\System32\en-US]
* netstat.exe.mui [C:\Windows\System32\en-US]

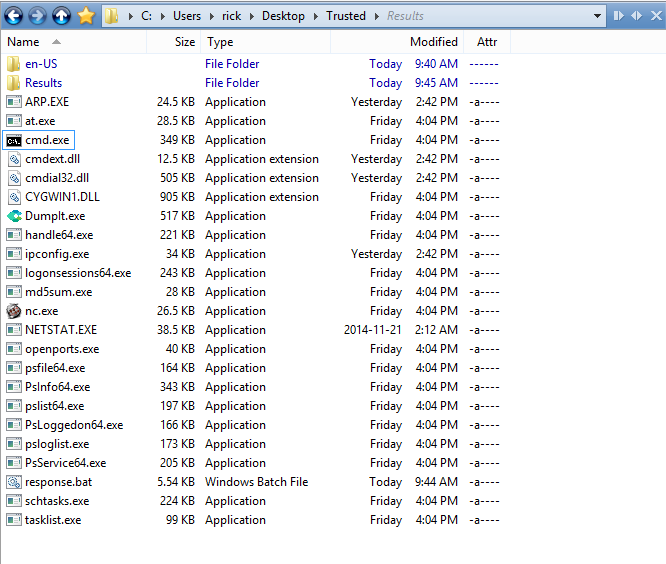
**Note:** In this case, you would not prepend the file names with **t\_**.



**Figure 6:**

Used with permission from Microsoft.

Once complete, your Trusted directory should resemble Figure 7.



**Figure 7:**

Used with permission from Microsoft.

1. Scripting Your Response

## Scripting Your LRK

The following script uses the hostname of the target computer as the filename for the output. This allows you to use the same target drive for multiple runs of the LRK. The script starts by running dumpit to capture memory and then runs the tools to capture the volatile information. The results from the tools are saved in the Results folder, and then the contents of the result folder are hashed using **md5sum**. There is a line of asterisks (\*) placed between the results of each command.

1. Open Notepad and type the following (feel free to try adding other commands).

Start of script

@echo off

hostname > tmphost

set /p hostvar= < tmphost

del tmphost

dumpit /T RAW /Q /N /O Results/%hostvar%.mem

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

echo Windows 7 Live Response

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

ECHO Date and Time [start] >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

date /t >> Results/%hostvar%.txt

time /t >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psloglist -s -x security >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psloglist -s -x security >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psloglist -s -x application >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psloglist -s -x application >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psloglist -s -x system >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psloglist -s -x system >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo netstat -an >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

netstat -an >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo netstat -rn >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

netstat -rn >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo openports -path >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

openports -path >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo pslist64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

pslist64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo tasklist /svc >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

tasklist /svc >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psloggedon64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psloggedon64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo handle64 -a >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

handle64 -a >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo logonsessions64 -p >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

logonsessions64 -p >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psinfo64 -h -s -d >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psinfo64 -h -s -d >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psfile64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psfile64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo psservice64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

psservice64 >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo at >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

at >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo schtasks >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

schtasks >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo ipconfig /all >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

ipconfig /all >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo ipconfig /displaydns >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

ipconfig /displaydns >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo arp -a >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

arp -a >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

echo Date and Time [end] >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

time /t >> Results/%hostvar%.txt

date /t >> Results/%hostvar%.txt

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* >> Results/%hostvar%.txt

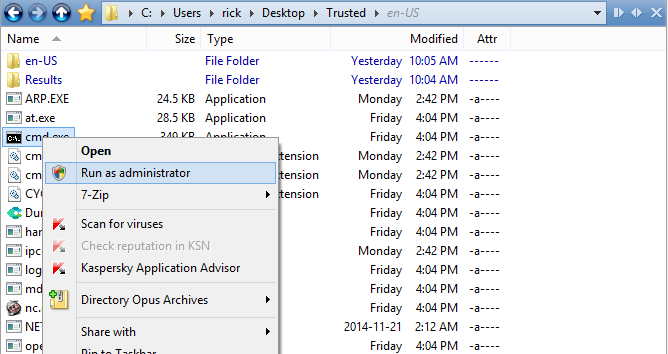
echo Calculating md5sum...

md5sum Results/%hostvar%.mem >> Results/%hostvar%\_mem.md5

md5sum Results/%hostvar%.txt >> Results/%hostvar%\_txt.md5

End of script

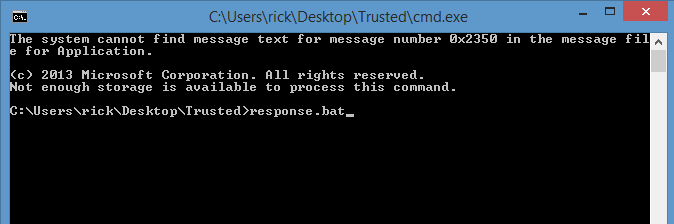
1. Save the file as **response.bat** to the Trusted directory.
2. Running the Script
3. Open the Trusted directory in File Explorer.
4. Right-click the **cmd.exe** file and select **Run As administrator**.



**Figure 8:**

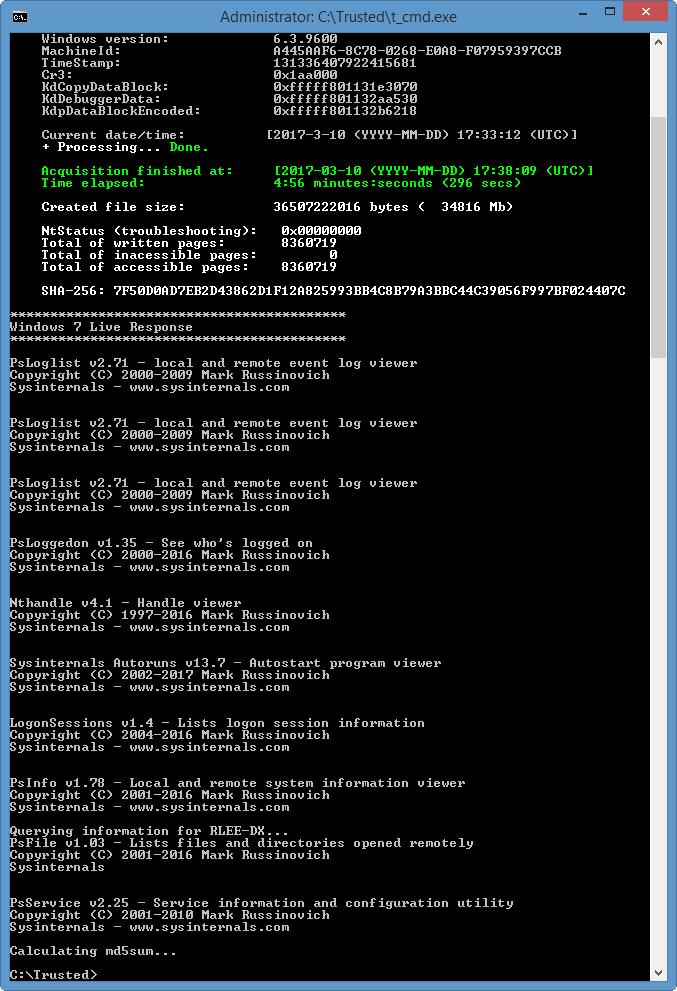
Used with permission from Microsoft.

1. In the command shell, type **response.bat** and press ENTER.



**Figure 9:**

Used with permission from Microsoft.



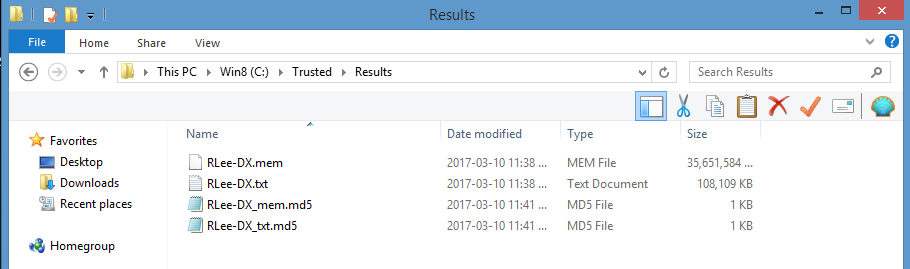
**Figure 10:**

Used with permission from Microsoft.

1. When your script has completed and the command prompt reappears, take the external drive that you ran the script from (containing your LRK) to the system on which you are running your analysis.
2. Navigate to the Trusted\Results directory using File Explorer.

The directory contains the information shown in Figure 11.

1. Move the .json file from the trusted directory to the Results folder. The file named <computer name>.json has the information from running the memdump file.



**Figure 11:**

Used with permission from Microsoft.

1. Save the files. You will refer to them in future modules.
2. Confirm that the folder contains the following five files:
3. <computer name>.json
   * Contains data collected during the running of dumpit
4. <computer name>.mem
   * Contains the raw memory dump from running dumpit
5. <computer name>.txt
   * Contains the results of the LRK
6. <computer name>\_mem>.md5
   * Contains the MD5 hash from <computer name>.mem
7. <computer name\_txt>.md5

* Contains the MD5 hash from <computer name>.txt