**Running the Incident Response Tools**

These incident response tools collect volatile data, RAM image, and a forensic image of Windows machines used for digital forensic investigation by your IT Security team. These tools run using simple batch commands which creates the files and then places the files into a folder with the hostname of the computer.

1. **Description**

The collection of data is accomplished by running three batch (.bat) files. This minimizes the collection digital fingerprint. The tools collecting data are broken down as follows:

**Batch file 01:** Collects volatile data from a live system. These are things that are lost once the computer is shut down and cannot be recovered.

1. Sysinternals

-Autorunsc

-Psfile

-PsInfo

-Pslist

-PsLoggedon

-Tcpvcon

1. Cprocess
2. Cports
3. Winaudit

**Batch file 02:** This collects data from the computers RAM

1. Winpmem

**Batch file 03:** This creates a compressed copy of the target computers hard drive. It creates files in an industry standard file system that is capable of being read by most any digital forensic software.

1. FTK Imager

The first two batch files are typically fairly small in size so collection should not be a problem. The third batch file using FTK Imager will compress the data into several “.E” files and will take up considerable space; 250GB files are not uncommon for a laptop computer with a 500GB hard drive.

To run the batch files you need to place the tools onto an external drive that can be written to. A USB drive works best. The tools themselves are only around 9 MB so even though a small flash drive will meet the needs for the tools a larger drive is recommended since the data collected will save to the same drive where the tools are located. If you understand how to read and rewrite scripts you can use one drive for the tools and another drive where the data will be stored.

This process is easiest if you place the files in the same drive you will use to save the forensic data. This may require a large storage drive since FTK Imager creates a copy of the target hard drive which can be up to 800GB or more

Install the tools and batch files on a drive without placing them into another folder (see image 1)

Graphical user interface, text, application

Description automatically generated

*Image 1*

1. **Running the batch files**

In Forensic work it is best if the suspected device is not shut down. The device is preferred to keep running so that the volatile data can be collected. Once a computer shuts down all the volatile data is lost forever. For security purposes, it is best to disconnect the device from the network however.

1. **Collecting data from a live device**

If the device is still running under standard user credentials do the following first steps

1. Open a command prompt as Administrator. Go to the start menu and type “cmd” (without quotes), right click and run as Administrator.
2. Next, with the USB that contains the Forensic tools, insert it into a USB port
3. Within the command window, change directors to the drive containing the USB (Example: F:)
4. Follow the instructions on running the batch files below
5. **Collecting data from a device that has been shut down**
6. Log into the target computer as an Admin.
7. Next, with the USB that contains the Forensic tools, insert it into a USB port
8. Open a command prompt. Go to the start menu and type “cmd” (without quotes), right click, and run as Administrator.
9. Within the command prompt change to the directory of the installed drive. (Example: F:)
10. Follow the instructions on running the batch files below

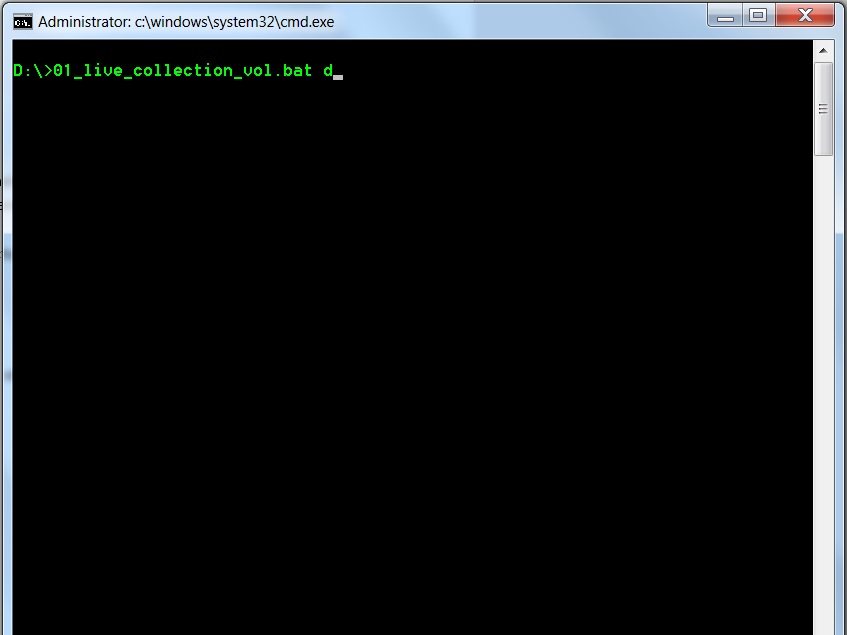
**Batch file 01:**

This script will collect the volatile data from a live system.

Syntax is as follows:

01\_live\_collection\_vol.bat [drive letter for tools and data storage]

example: 01\_live\_collection\_vol.bat D (see image 2)



*Image 2*

After running this first batch .bat file, it creates a folder with the name “Data-“ and the computer system name and places the collected data into the file. Each .bat file will place the collected data into the new folder. (see Image 3)

Graphical user interface, table

Description automatically generated

*Image 3 – notice the folder called Data-LAZYSPROCKET-DE*

Open the folder and open the folder “volatile\_data.” If everything worked correctly there should be several files. It is best to verify that all of the files have data but a good check is to open the file called, “psloggedon-YourComputerName” because this one should always have data while the others may or may not have data depending on the computer. If everything looks good then please go to batch file two.

**Batch file 02:**

This script only collects one file for memory analysis. The syntax is similar to the first one. The file will be stored in “Data-YourComputerName\mem\_image.” Just check to make sure the .bin file is there.

02\_live\_collection\_ram.bat d

**Batch file 03:**

The final script will collect an image of the computer hard drive. It compresses the image into several smaller “.E01” files. The collection of the forensic image will take much longer than the first two. For example, a 2TB hard disc took around 7 hours to complete. It created 387 smaller .E01 files but they are compressed into 771GB. These are the files that will be loaded into a Forensic analysis tool such as Encase, FTK, Autopsy or other forensic software. If any files are missing or corrupt they will not load into the Forensic software so care must be taken to not interrupt the collection.

There are a couple of extra steps for collection and is described below.

1. Obtain the drive number of the target drive. In the command window change directories to where the ftkimager.exe is located: E:\IR\_tools\IR\_tools\ftkimager (see image 4)
2. Type the following into the window: ftkimager.exe –list-drives (see image 4)

Text

Description automatically generated

*Image 4*

In the image there are three drives. Physical drive 2 is obviously a 31GB USB drive so we don’t want this one. Physical drive 1 is the drive I am using for the tools and collecting the data; it is 2TB SCSI. This means Physical drive 0 is the computer hard drive and this is the one we need to collect an image.

1. Type the following into the window: 03\_live\_collection\_drive.bat E 0

“E” is the drive for my tools

“0” is the computer hard drive to collect the forensic image

(See Image 5)

Text

Description automatically generated

*Image 5*

Once it completes you will get a prompt. Follow the instructions and then go into the folder drive\_image and verify there are several “.E0” files (Images 6 and 7)

Text

Description automatically generated

*Image 6*

Table

Description automatically generated

*Image 7*

1. **Send all the files to the Forensic Analyst or the IT Security team**