Memory capture for Windows OS

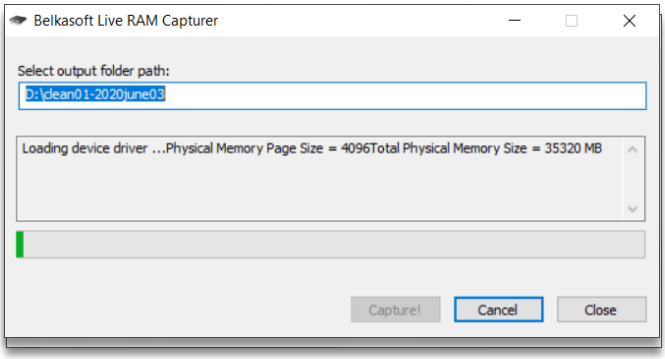
Note: We will first acquire live memory (RAM) from a Windows system based on the concept of "Order of Volatility" which states that more volatile data must be acquired before acquiring other data that may be less volatile. Live memory of a system i.e. the RAM is more volatile than the data on the hard disk(s) so it must be acquired first. **Failure to do so may result in the loss of key evidence.**

1 Preparation (on standalone machine)

1. "Belkasoft RAM Capturer" is a free imaging tool designed to capture the physical memory of a suspect's computer, allowing investigators to recover and analyse valuable artifacts that are often only found in memory. 32- and 64-bit versions of this may be downloaded from: https://belkasoft.com/ram-capturer . Select the version that matches the architecture of the target machine.
2. Ensure that you have compression software capable of creating encrypted ZIP archives available in your system. If not, IBM Security X-Force IR recommends using 7-Zip Portable, available from the official website: http://portableapps.com/apps/utilities/7-zip_portable or any other tool of your choice.
3. Prepare external storage media, with at least the same capacity as the size of the RAM in the target machine. This storage media will be used to store the forensic image of the RAM created by Magnet RAM Capture. Perform a quick format of the external storage media with the NTFS file system - all data on this media may be irrecoverably lost! If it is not possible to use external storage media, a network share can be used as an alternative.
4. Copy "MRCvXXX.exe" and if necessary "7zip Portable" on to the external storage media.

2 Acquiring live Memory (on target machine)

1. Connect the external storage media to the target machine.
2. Execute the Belkasoft RAM Capturer icon to start the program.
3. In Belkasoft RAM Capturer, enter a destination path for the memory image file. **IMPORTANT**: This should be on the external media connected to the target Windows system **NOT** the target device. You are only required to specify a folder path; no filename is necessary.
4. Click the **"Capture!"** button on the same screen to begin the live memory acquisition process.



5. At the end of the process, you will have the memory dump file created in the desired folder on the external media.
6. Disconnect the external storage media from the target machine.

3 Preparation for delivery to IBM Security X-Force IR (on standalone machine)

1. Disconnect the external storage media from the target machine.
2. Connect removable media to a standalone workstation.

3.1 Calculate hash value

Note: In the following commands, replace 'ram_image_file' with the path to the previously created RAM image file.

3.1.1 Using Linux

To calculate hash values on a Linux machine, launch a shell (most probably bash) and execute the following commands:

```
$ md5sum ram_image_file >> memory_image_checksum.txt
$ sha1sum ram_image_file >> memory_image_checksum.txt
```

3.1.2 Using Mac OS X

To calculate hash values on Mac OS X machine, launch shell (most probably Terminal) and execute the following commands:

```
$       shasum       ram_image_file       >>
memory_image_checksum.txt
$        md5        ram_image_file        >>
memory_image_checksum.txt
```

3.1.3 Using Windows

To calculate a hash value on a Windows machine, launch Windows PowerShell and execute the following commands:

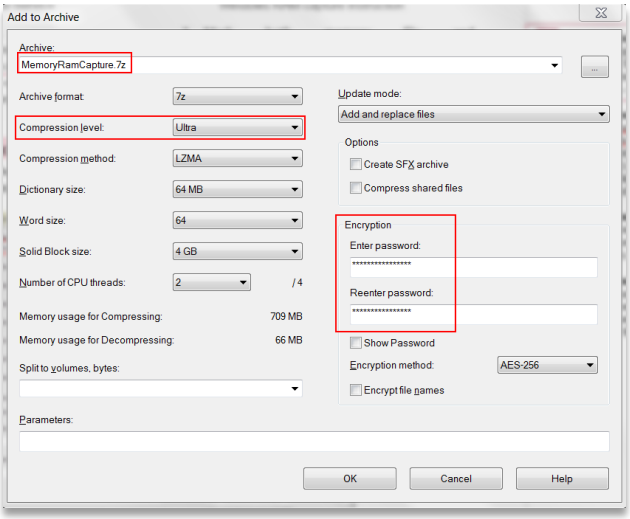
```
Get-FileHash ram_image_file -Algorithm MD5
>> memory_image_checksum.txt
Get-FileHash ram_image_file -Algorithm SHA1
    >> memory_image_checksum.txt
```

3.2 Verify Hash output

Check whether the output file 'memory_image_checksums.txt' contains the calculated hash values. If everything is fine, place the output file memory_image_checksum.txt in the same location as the memory image.

3.3 Compress and encrypt

1. Copy the file 'memory_image_checksum.txt' to the same location as the RAM capture.
2. Create a compressed and encrypted archive with the below options using 7-Zip Portable.
3. Open the folder containing the dump file and select both the memory dump file and 'memory_image_checksum.txt'.
4. Provide a suitable filename for the archive, set compression level to maximum, enable encryption with complex password (at least 16 characters, mixed case letters, numbers, and special symbols), as shown on the screen shot below.



5. After encryption is completed, test the archive by using 7-Zip to open the newly created file with 7z extension, provide the password and click 'OK', then click 'Test' from toolbar. If the test completes without errors, encryption was successful.
6. If archive testing was successful, encryption was successful. Original file should be securely wiped, using your organisation's approved method.

3.4 Delivering evidence to IBM Security X-Force IR

1. The compressed archive is now ready for delivery to IBM Security X-Force IR via agreed method of delivery.
2. Share the complex password used for encryption with IBM Security X-Force IR using a different communication channel than used to share the forensic image.
3. Should you have any questions on this step, please contact the IBM Security X-Force IR consultant who requested the evidence.