Windows RAM capture instruction

1 Preparation (on standalone machine)

1. Download all RAM capture software listed below which is recommended by IBM X-Force IRIS and proceed with this manual or use any other software of your choice and follow instruction of that provider. Below you will find download instructions for:
   a. Belkasoft Live RAM Capturer
   b. Magnet RAM Capture
   c. MoonSols DumpIt
2. Ensure that you have compression software capable of creating encrypted ZIP archives available in your system. If not, IBM X-Force IRIS recommends using 7-Zip Portable, available from official website: http://portableapps.com/apps/utilities/7-zip_portable or any other tool of your choice.
3. Find removable storage media:
   a. ensure that the its capacity is larger (not equal) that amount of RAM memory of target machine,
   b. it will be formatted and data may be irrecoverably lost!
4. Prepare removable media:
   a. Format the media (quick format is sufficient) using NTFS or ExFAT filesystem.
   b. Copy all downloaded software onto the media.
   c. If it is not possible to connect external storage media, network shared can be used as an alternative.

1.1 Belkasoft Live RAM Capture

'Belkasoft Live RAM Capturer' is available in 32 or 64 bit versions. Choose version matching OS bit version of target machine. It can be obtained from vendor website: www.belkasoft.com. It is required to provide contact details to receive a download link.

1.2 Magnet RAM Capture

It can be obtained from vendor website: www.magnetforensics.com. It is necessary to provide contact details to download software, but the download starts after submitting the form.

1.3 MoonSols DumpIt

It can be obtained from vendor website: https://my.comae.com/tools.

2 Information capture (on target machine)

It is **required is to have administrative rights on the machine**. Results of only one of the tools are required, but 3 options are provided in case of problems with any of them. Use the tool recommended by IBM X-Force IRIS consultant. If no tool was recommended, please use Belkasoft Live RAM Capture.

1. Connect prepared previously removable media.
2. Launch chosen tool.
3. Choose output folder for a capture file on the connected storage media. **IMPORTANT:** Do not store RAM image file on any internal storage of target system, always create it on removable media.
4. Click Capture/Start button.
5. When completed, close application and safely disconnect media from the system.

3 Preparation for delivery to IBM X-Force IRIS team (on standalone machine)

3.1 Connect removable media to a workstation

If a storage media is a USB drive, it is possible, that it has become infected. To limit chance of spreading potential infection, this stage should be performed on a different type of operating system, than the one which is being analyzed, eg. if RAM capture was done on Windows, storage media should be connected to the Linux or OS X system.

When plugging it into a clan system special caution is necessary:

1. autorun feature for removable media should be disabled,
2. system should be fully updated,
3. antivirus scan of a media with updated signature set should be performed.

3.2 Calculate hash value

3.2.1 Using Linux

To calculate hash values on Linux machine, launch shell (most probably bash) and calculate checksums of a file using following commands, redirecting output to the file:

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

3.2.2 Using Mac OS X

To calculate hash values on Mac OS X machine, launch shell (most probably Terminal) and calculate checksums of a file using following commands, redirecting output to the file:

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

3.2.3 Using Windows

To calculate a hash value, perform following steps:

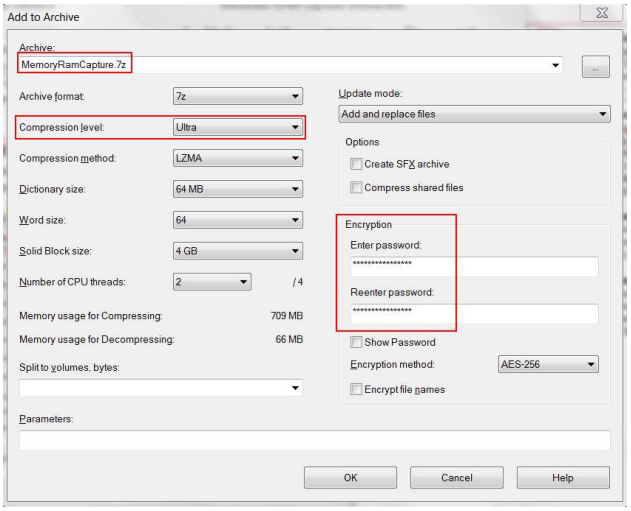
1. Download Microsoft File Checksum Integrity Verifier from https://support.microsoft.com/en-us/kb/841290
2. Extract downloaded file.
3. Launch cmd.exe and navigate to the folder containing extracted fciv.exe
4. Run command: `fciv.exe -md5 -sha1 ram_image_file > memory_image_checksum.txt`

3.3 Verify Hash output

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

3.4 Compress and encrypt

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



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

3.5 Delivering file to IRIS Team

1. Compressed archive and text file are ready for delivery to IBM X-Force IRIS team via agreed method of delivery.
2. Share complex password used to for encryption with IBM IRIS team using different communication channel then used to share forensic image.