Windows RAM capture instruction

1 Preparation (on standalone machine)

1. Download winpmem from official Rekall Releases website: http://releases.rekall-forensic.com/. The latest version at the time of writing this guide is winpmem-2.1.post4.
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.

2 Information capture (on target machine)

It is **required is to have administrative rights on the machine**.

1. Connect prepared previously removable media.
2. Launch windows commands shell with administrator rights.
3. Navigate to the storage media and folder containing downloaded tools.
4. Initiate memory dump process as stated below, please use hostname in the output file name:

```
winpmem-2.1.post4.exe –o <hostname>.aff4
```

5. When completed, close command shell 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

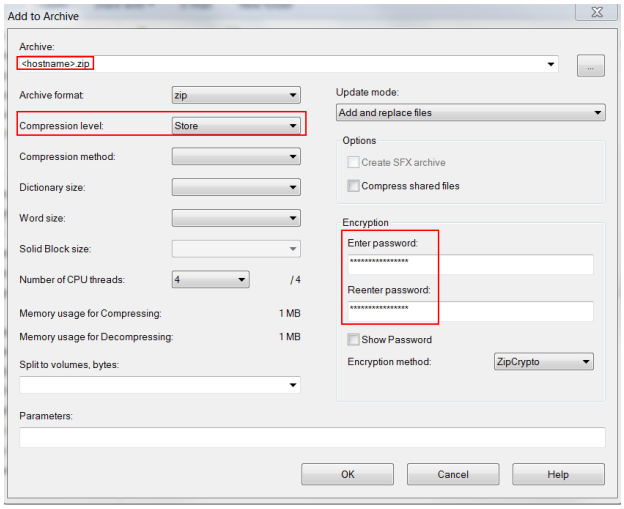
If a storage media is a USB drive, it is possible, that it has become infected. To limit chance of spreading potential infection, this stage should be performed on a different type of operating system, than the one which is being analyzed, eg. if RAM capture was done on Windows, storage media should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

1. Create compressed encrypted archive with below options, eg. using 7-Zip Portable.
2. Open the folder containing *.aff4 file and select this file.
3. Fill in filename, set compression level to “store” (aff4 is already compressed), enable encryption with complex password (16 characters, mixed case letters, numbers, and special symbols), as shown on the screen shoot below.



4. After encryption is completed, open newly created archive, provide password and click ‘OK’ button, then click ‘Test’ from toolbar. If test completes without errors, encryption was successful.
5. If archive testing was successful, encryption was successful. Original file should be securely wiped, using your organization approved method.

3.3 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.