1 Preparation

1. Obtain administrative credentials necessary to work with VMs on ESXi/vSphere.
2. Ensure that you have enough storage on ESXi cluster to store and compress extracted files (especially disk images) or provide additional storage in a form of USB drive or network share.
3. Do not power off target VM. Create a snapshot of a target VM (ensure that RAM is included in the snapshot). Both RAM acquisition and Disk image acquisition will be performed based on created snapshot.
4. Identify which sequence number is related to created snapshot by finding a snapshot name in *.vmsd file for target machine – this will be probably the highest sequence number.

2 RAM acquisition

1. Navigate to the folder containing VM files.
2. Extract (copy out) *.vmem file related to created snapshot. If there is no *.vmem file, then there should be *.vmss or *.vmsn files. Extract those ones which are related to the created snapshot.

3 Disk image acquisition

1. Create a clone from previously created snapshot. Clone VM will be automatically placed in a powered off state, so there is no need to place it in an isolated network. Clone will not contain any snapshots.
2. Navigate to folder which stores files of a clone.
3. Extract all disk *.vmdk files.

4 Preparation for delivery to IBM X-Force IR team (on standalone machine)

ESXi is a Linux system, so standard system tools can be used to calculate hash value from system command line.

Split RAM files (*.vmem, *vmss, *.vmsn) and disk files (*.vmdk) into 2 directories (called 'ram' and 'disk'). Proceed with below instruction depending on which files you were asked to extract.

4.1 Calculate hash of RAM files

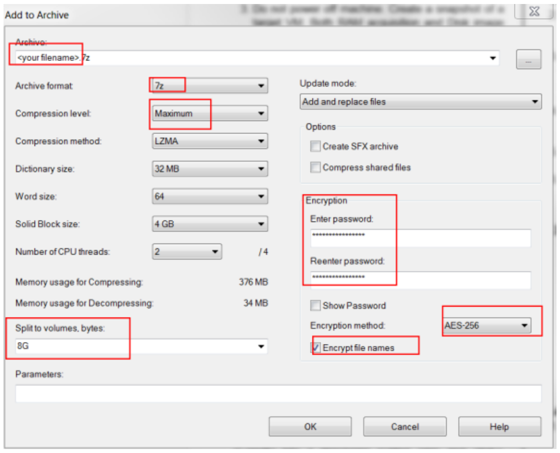
1. Navigate to 'ram' folder.
2. Calculate hash values:
```
$ sha1sum ./* > ram_sha1_hashes.txt
```

4.2 Calculate hash of disk files

1. Navigate to 'disk' folder.
2. For each *.vmdk file calculate hash value:
```
$ sha1sum ./<file_name>.vmdk > <file_name>_sha1.txt
```

4.3 Compress and encrypt files

1. Copy out all collected files from ESXi storage to a separate machine which you can use for delivery to IBM X-Force IR team.
2. Ensure that you have compression software capable of creating encrypted ZIP archives available in this system. If not, IBM X-Force IR 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. Compress whole 'ram' folder into single archive (ensure that you include ram_sha1_hashes.txt), and each vmdk together with its hash file (*_sha1.txt) into separate archives. For each archive to be created follow below steps.
   a. In 'Add to Archive' window choose '7z' from 'Archive format' dropdown menu, choose 'Maximum' from 'Compression level' dropdown menu, set up split into 8GB files, enter complex (16 characters, mixed case letters, numbers, and special symbols) password in 'Enter password' and 'Reenter password' fields, choose 'AES-256' from 'Encryption method' dropdown menu and tick 'Encrypt file names' checkbox, and click 'OK' button.



Archive: <your filename>.7z

Archive format: 7z

Compression level: Maximum

Compression method: LZMA

Dictionary size: 32 MB

Word size: 64

Solid Block size: 4 GB

Number of CPU threads: 2 /4

Memory usage for Compressing: 376 MB

Memory usage for Decompressing: 34 MB

Split to volumes, bytes: 8G

Parameters:

Update mode: Add and replace files

□ Create SFX archive

□ Compress shared files

Enter password: ****************

Reenter password: ****************

□ Show Password

Encryption method: AES-256

☑ Encrypt file names

b. 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. <u>If test completes without errors, encryption was successful.</u>

c. Use method approved within your organization to <u>securely erase original files extracted from VM</u>.

4.4 Delivering file to IR Team

1. Collected files are ready for delivery to IBM X-Force IR team via agreed method of delivery. Created clones and snapshots can be.
2. <u>Share complex password</u> used to for encryption with IBM IR team <u>using different communication channel</u> then used to share forensic image.