1 Preparation (on standalone machine)

Prepare storage media, with at least double the size as media in target machine (or two media, each at least the same size as media in target machine). Tool allows forensic images to be stored on external hard drive attached to target machine. Perform a quick format of a storage media to a filesystem which can handle 4GB files – all data on this media may be irrecoverably lost!

2 Information capture (on target machine)

It is required is to have administrative rights on the machine. Connect prepared previously removable media (if prepared 2 media, connecting only one is sufficient).

1. Gain root rights and change directory to removable media.
2. Create disk image using following command:

```
# dd if=/dev/DRIVE_NAME bs=4K
conv=sync,noerror | tee <hostname-
drive>.dd | sha1sum > <hostname-
drive>.dd.sha1
```

3. When completed, safely disconnect media from the system.

Note: while creating image with DD, there is no progress shown on the console and it can take several hours.

3 Image conversion

This process requires Linux system, with ‘ewftools’ (or ewf-tools) package installed, which should be available from standard repositories for most Linux distributions.

Connect storage media (in case of using two media, connect both of them). Use second media to store output files created in below steps:

1. Convert DD image:

```
$ ewfacquire -c best -d sha1 -f ewfx -u -
S 4G -t /DST_DIR/<hostname-drive>
/SRC_DIR/<hostname-drive>.dd
```

   When finished, multiple *.e01, *.e02, etc files will be created in destination directory.
2. Verify created image. Make sure that he results is “SUCCESS” and both hash pairs, MD5 and SHA1 in the output are equal:

```
$ ewfverify /DST_DIR/<hostname-drive>.e01
-d sha1
```

3. Verify that the SHA1 hash value in E01 image is equal to SHA1 hash value from raw image, by comparing hash values from 2 below commands:

```
$ ewfinfo /DST_DIR/<hostname-drive>.e01 |
grep SHA1
$ cat /DST_DIR/<hostname-drive>.dd.sha1
```

4. Encrypt captured data with complex password (16 characters, mixed case letters, numbers, and special symbols):

```
$ gpg --symmetric --cipher-algo AES256
/DST_DIR/<hostname-drive>.e01
```

   Due to data storage format, it is sufficient to only encrypt *.e01 file. This step will create *.e01.gpg file.
5. Use method approved within your organization to securely erase *.dd and *.e01 files (but NOT *.e01.gpg).

4 Delivering files to IBM Security X-Force IR

1. Following files should be delivered to the IBM Security X-Force IR team via agreed method of delivery: *.sha1, *.e01.gpg, *.e*,
2. Share complex password used to for encryption with IBM Security X-Force IR team using different communication channel then used to share forensic image.