Imaging a Target Computer

Introduction

This guide covers how to image a target computer and other storage devices.

This document applies to the following applications		
ADF PRO	Digital Evidence Investigator	

What is a Forensic Image?

A forensic image is a copy of a target storage device usually created to preserve the original device. Some forensic images contain all the bits of information of the target storage device and require additional processing to interpret the raw data into a file system. These are usually called physical images. The two most common formats of physical images are DD and Expert Witness Format (EWF).
Some forensic images contain the file system of the target storage device instead of the raw data. These are usually called logical images. The most common format of logical images is zip.

Write-Protection

It is highly recommended to use a write-blocker whenever connecting a target storage device for imaging. Write blockers allow reading but prevent writing data to a target storage device. When using the Collection Key to reboot a target computer, a software write-blocking method is automatically used. When using the Collection Key to scan a live target computer, or the remote agent, no write-blocking method can be used as the computer needs write permission to operate.

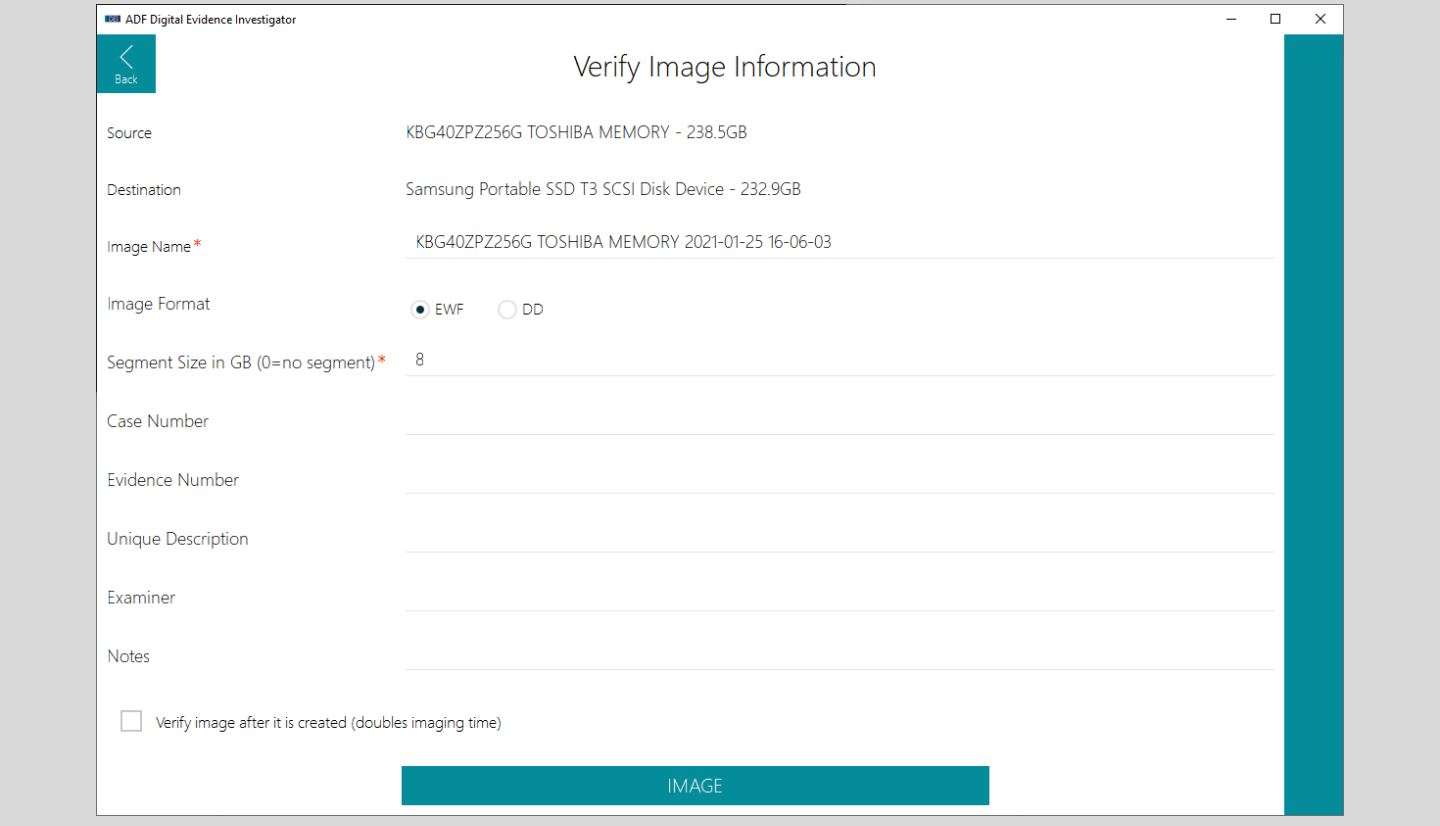
Imaging from the Collection Key

It is possible to image the drives of a running or rebooted computer from the Collection Key. See the Rebooting a Computer guide on how to reboot a computer with the Collection Key.

Here are the instructions to image the computer when running from the Collection Key:

1. Navigate to **Home > Image Computer**.
2. Select the physical storage device to image from the list.
3. Connect the destination drive. It should be detected automatically. If not detected, unplug it and try again. The destination drive should be as big as the source drive and formatted with a NTFS file system.

4. Verify the source and destination and enter some information:

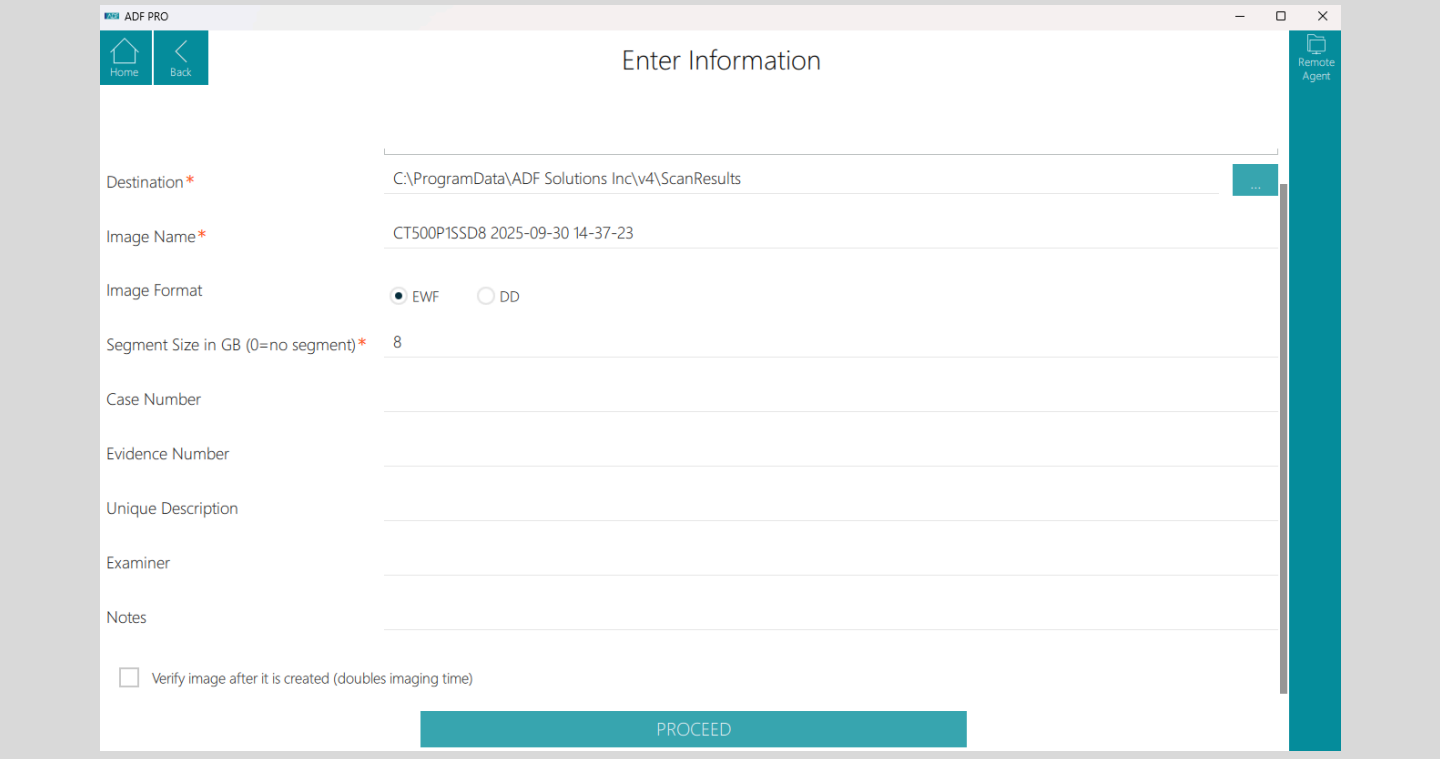


   a. **Image Name**: the name of the image and user defined.
   b. **Image Format (physical image)**:
      i. DD creates a raw copy of the source drive. It creates file segments of at most 4GB.
      ii. EWF creates an Expert Witness Format copy of the source drive. It uses a compression ratio of 1 (low compression and fast) and creates file segments of at most 4GB.
   c. **Segment Size in GB (0=no segment)**: the size of each segment to split a large image into smaller files. Entering 0 creates only one file for the entire image.
   d. **Case Number**, **Evidence Number**, **Unique Description**, **Examiner**, and **Notes** are text fields that are optional and are added to the image log file.
   e. **Verify image after it is created**: this option will read the image file segments upon completion, compute their global hash value, and compare it to the hash calculated during the imaging process. ADF recommends selecting this option whenever possible.
5. When ready, click on the **PROCEED** button to start imaging.
6. A progress screen is displayed indicating the time elapsed and remaining. It is possible to cancel the imaging process.
7. If the image is to be verified, this will occur after the imaging process and a new progress bar will be displayed.

If canceling the imaging process before it completes, the image file segments are preserved. Missing segments are likely to render an EWF image unusable, whereas a DD image might still be usable, though incomplete.

Imaging from the Desktop Application

Here are the instructions to image an attached or remote device when running the desktop application:



1. Navigate to **Home** > **Investigate Device** > **Image** (DEI PRO **& with an active External Devices license add-on** MDI)
2. Select the storage device to image directly in the **Source** dropdown menu or by using the **Remote Agent** buttons.
    a. The **Remote Agent** procedure is described in the Connecting a Mac/Windows Target Computer with the ADF Workstation chapter in the Scanning a Target guide. This creates a logical image.
    b. The **Source** dropdown shows the connected storage devices.
        i. Note that in MDI, with an active External Devices license, it is possible to image external devices such as USB thumb drives, USB external hard drives, external SSDs, external optical drives (if supported), and external card readers (if supported).
3. Enter the rest of the information as described above.

Make sure proper write-blocking measures are in place to protect the attached device.

Imaging from the Scan Progress Screen

It is possible to image the scan targets without going back to the Home screen.

From the scan progress screen, click on the **IMAGE** button. This will stop the scan and start the imaging process described above.

Physical Image File Structure

The image file segments are saved at the root of the destination drive:

- Image Name - folder named after the image name.
    - Image_name.ext - image file segment where ext can be e01, e02, etc or 001, 002, etc.
    - Image_name.log - the log file

Physical Image Log File

A log file is created at the end of the imaging process and saved with the image file segments. Here is an example of such log file:

```
Created By ADF Digital Evidence Investigator 2.2.1

Case Information:
Case Number: ABC123456
Evidence Number: EV112233
Unique Description: SD card found connected to target computer
Examiner: Bob A.
Notes:

Physical Drive Information:
Drive Model: SDXC Card
Drive Serial Number: 201209010309
Drive Interface Type: USB
Removable drive: True
Source data size: 61056 MB
Sector size: 512 B
Sector count: 125042688

Image Information:
Imaging started : Fri Jun 19 13:02:09 2020
Imaging finished : Fri Jun 19 13:22:58 2020
Format: EWF (e01)
Segment size: 4.0GB max
Compression level: LIBEWF_COMPRESSION_FAST

Segment list:
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E01
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E02
```

```
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E03
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E04
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E05
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E06
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E07
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E08
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E09
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E10
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E11
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E12
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E13
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E14
E:\SDXC Card 2020-06-19 13-01-40\SDXC Card 2020-06-19 13-01-40.E15

Physical Drive Hash Values:
MD5 checksum: 610a095a5ad455b4a68892d785736267
SHA1 checksum: 587467798386f3622275ac15a979bdeaf198f27b
```

Logical Image File Structure

When acquiring a logical image from the remote agent, an ADF data container is created. The format of the data container is described in the ADF Data Container Structure guide.