Module B0: Create Disk Image with FTK Imager

Pre-requisite Knowledge and Skills:

1. Understand the basic of Computer Operations

Learning Objectives

1. Be familiar to disk image creation by using FTK Imager.

Recommended Running Environment/Tools:

- 1. Windows OS
- 2. AccessData FTK Imager
- 3. Write blocker

Material:

1. A Thumb Drive

Video Lecture:

1. N/A

Lab Assessment:

1. N/A

Acknowledgement:

Lab Instructions (missing the Write Blocker for demonstration purpose only):

- Plug in the thumb drive to user's computer. (Please note that this instruction is not forensically sound. For evidence to be forensics sound/court admitted, the evidence media, for example, thumb drives, hard disks, should be connected to a software or hardware write blocker first. The write blocker can intercept all communication between the evidence media and evidence acquisition tool/equipment which can prevent writing data to the evidence media. For more details on write blocker, please refer to https://www.forensicswiki.org/wiki/Write_Blockers. For a live demonstration on how to make a disk image, please watch YouTube video provided by Mr. Chuck Decastro https://www.youtube.com/watch?v=0kT7cAh9elE)
- 2. Run FTK image Recorder FIG Image 42.01 For Main Energy Action and Action

3. Click on file and select the create disk image function



- 4. Select physical drive option and click on next
- 5. Make sure to select the small-sized usb drive (note that your C drive usually is the default selection, please navigate the list to select the correct drive), and then click on finish

Select Drive	×
Source Drive Selection Please select from the following available drives: [I_PHYSICALDRIVE1 - General UDisk USB Device [IGB USB] I_PHYSICALDRIVE1 - General UDisk USB Device [IGB USB]	
< Back Finish Cancel Help	

6. On the new window, please click on the add option

Create Image		×	
Image Source			
\\.\PHYSICALDRIVE1			
	Starting Evidence Number:	1	
Image Destination(s)			
Add	Edit	Remove	
	Add Overflow Location		
		·	
✓ Verify images after they a	re created Precalculat	e Progress Statistics	
Create directory listings o	f all files in the image after the	y are created	
	Start Cancel		

7. Select the .e01 option (Encase format), or the .dd format (raw disk image, no meta data)

Select Image Type	×
Please Select the Destination Image Type	
O Raw (dd)	
◯ SMART	
(E01	
AFF	
< Back Next > Cancel	Help

8. Click next, and then fill in the optional information, and then click next

cube maniberr	001
Evidence Number:	001
Unique Description:	to create ADS disk image file
Examiner:	K12
Notes:	an ADS test image

9. Choose the desired image file name (ADS Image, for example), and select the correct directory where the disk image file will be created.

elect Image Destination	Browse For Folder
Image Destination Folder C:\Users\tu15\Desktop Browse	Select the destination folder for the image
Image Filename (Excluding Extension) ADS Image Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment Compression (0=None, 1=Fastest,, 9=Smallest) 6 Use AD Encryption	
< Back Finish Cancel Help	Make New Folder OK Cancel

10. Click on finish

	\times
Starting Evidence Number: 1	
Edit Remove	
Add Overflow Location	
e created Precalculate Progress Statistics	
all files in the image after they are created	
Start Cancel	
	Starting Evidence Number: 1 Simage [E01] Edit Remove Add Overflow Location e created Precalculate Progress Statistics all files in the image after they are created Start Cancel

11. Click on start option, you will create a disk image with extension E01, depends on the size of the disk, it could be a few minutes to hours.

Image Courses		DIVE1		
inage source.	II. (FITT STCALD)			
Destination:	C:\Users\tu15\Desktop\ADS Image			
Status:	Creating image.	•		
Progress				
Ela	psed time:	0:00:04		

12. When finishing, it should look like what shown below. This will create disk creation report, and verify whether the hashes of the disk image and original disk are the same (if same, verified).

nage Source:	\\.\PHYSICALDRIVE1		Computed bash	5317600d21601ba735e7e107fff1fbe2
-	C:\Users\tu15\Deskton\ADS Image		Stored verification hash	5317600d21601ba735e7e107fff1fbe2
counddon.	ci loseis (aro posició) pas inage	vith	Report Hash	5317600d21601ba735e7e107fff1fbe2
atus:	Image created successfully		Verify result	Match
Progress			□ SHA1 Hash	
			Computed hash	94f53ab03848408365b547e88fa7f00d70
			Stored verification hash	94f53ab03848408365b547e88fa7f00d70
Elar	osed time: 0:01:12		Report Hash	94f53ab03848408365b547e88fa7f00d70
Fsti	mated time left:		Verify result	Match
250			Bad Blocks List	
	Class		Bad block(s) in image	No bad blocks found in image

- 13. At the directory, you will find two files, ADS Image.e01 (disk image file) and ADS Image.E01.txt (verification file)
- 14. Close the FTK Imager.