DIGITAL FORENSIC CREATE DEVICE IMAGE USING FTK

MoTech IT Articles

NOEL MOSES MWADENDE

ABOUT THE AUTHOR.

Noel Moses Mwadende is the passionate book and article writer based of different books and articles concern computer science in general, especially in cybersecurity and machine learning, currently Noel is employed as youtuber and book author at MoTech which is mini firm dealing with provision of information technology services.

INTRODUCTION

To be honest forensic is the one of computer security field which is mostly seemed in positive way by major of people as it helps in investigation of different things happening in the society especially crimes.

Forensic have many direct advantages to the society and this is my driving force towards writing this simple guide on how to create disk image when doing device forensic, USB image is created as an example during device forensic.

The following below are the steps towards creation of USB disk image by using FTK image creator, make sure FTK is installed in your computer, let us go together below are the steps.

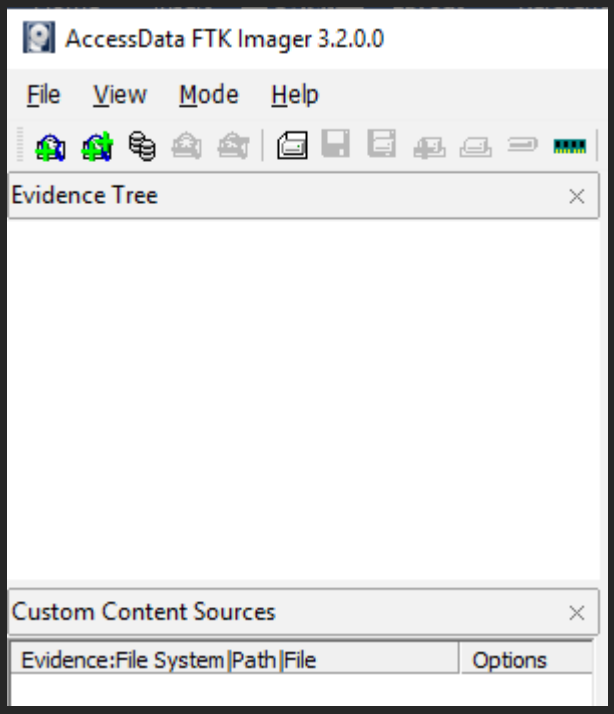

Fig. 1.

As shown in the figure 1 on the left side, select file, then choose create disk.

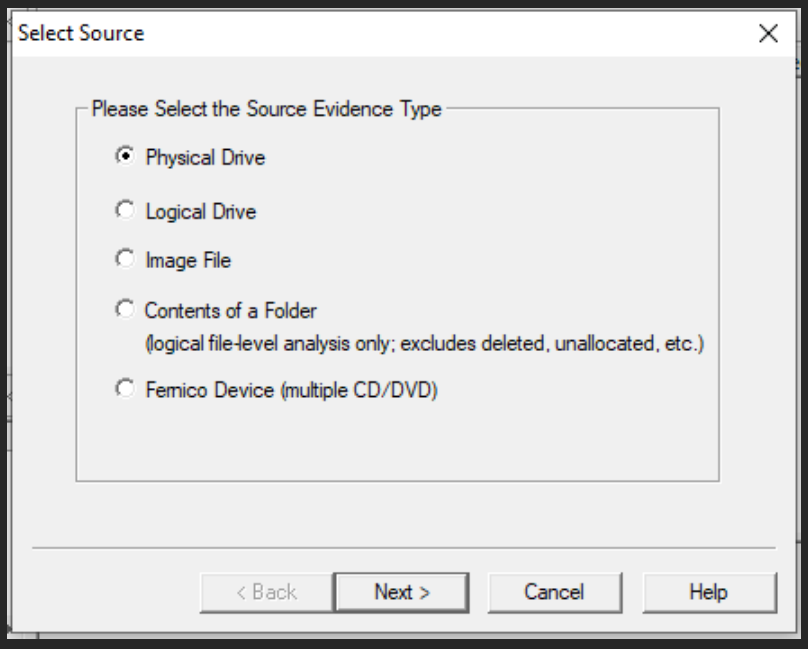

Fig. 2.

After clicking on the file, choose create disk option, after that new window will come which look as shown in the figure 2.

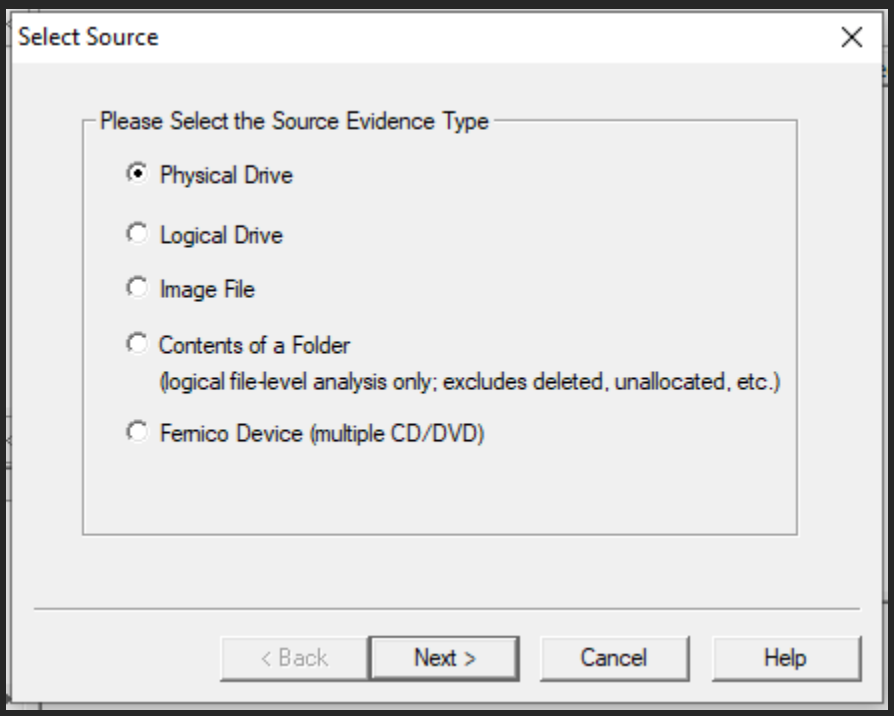

Fig. 3.

Select option number one which is Physical Drive as shown in the figure 3 and then click next present on the bottom of the figure.

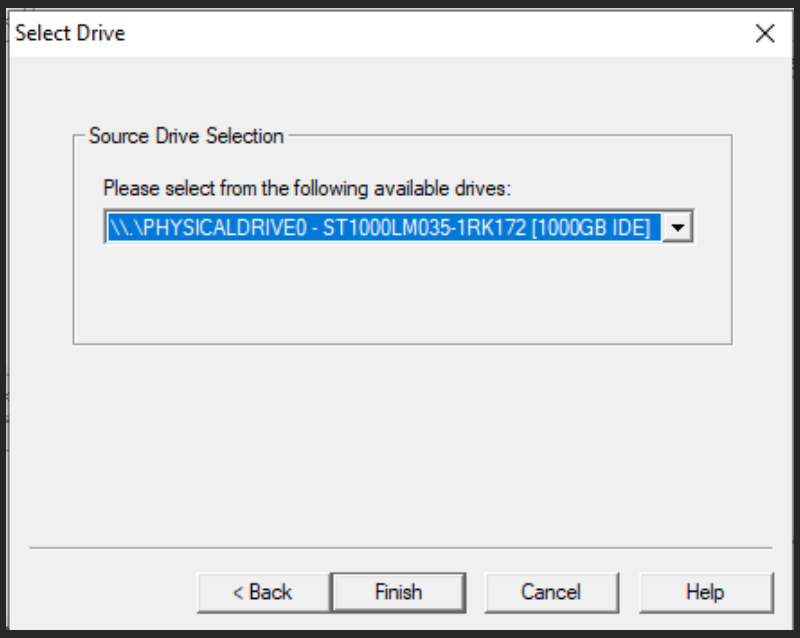

Fig. 4.

In the figure 4 shows all available drives, click and choose USB drive for creating image.

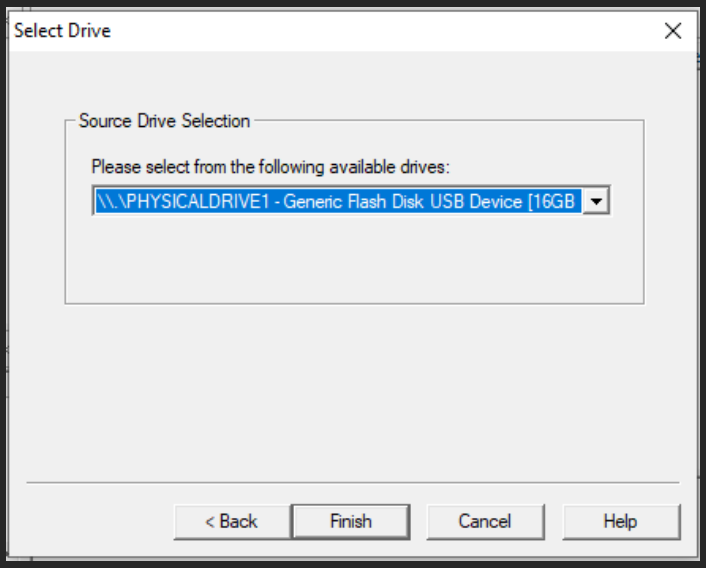

Fig. 5.

As shown in the figure 5, USB Device with size of 16 GB is created, finally you have to select finish.

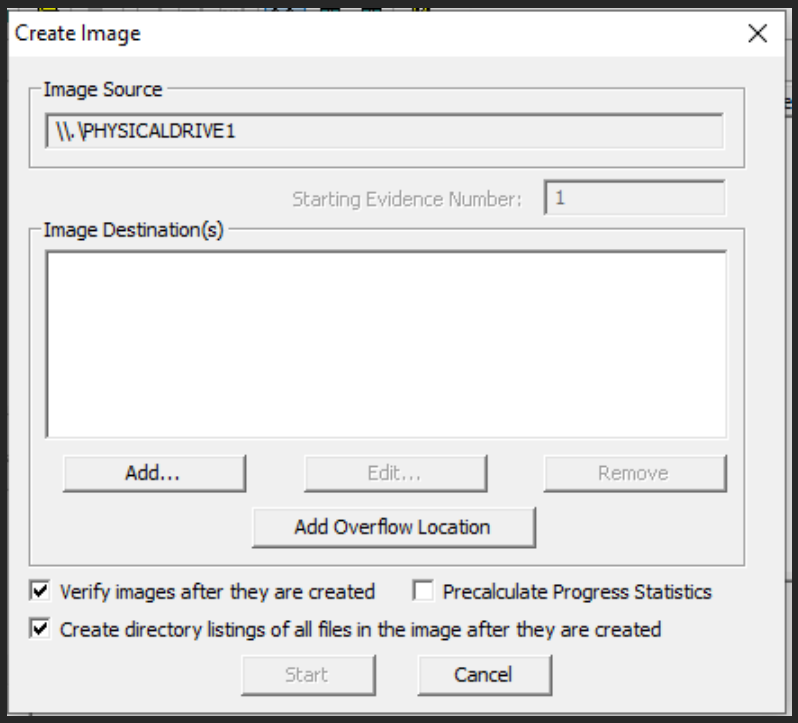

Fig. 6.

After clicking finish, new window will appear as shown in the figure 6, the following are the few description of the options shown in the figure 6,

Image Source ➔ is the place from which disk image is created.

Add ➔ is for add image format we want to create, this option depends on platform you are running this application, dd is mostly used in open source like Linux, EO1 and SMART are used in window, but for the time being choose EO1.

Verify images after they are created ➔ FTK imager will generate md5 and Sha1 to verify the created image if is correct.

Create directory listing of all files ➔ This will create all subdirectories and files in a single organized file.

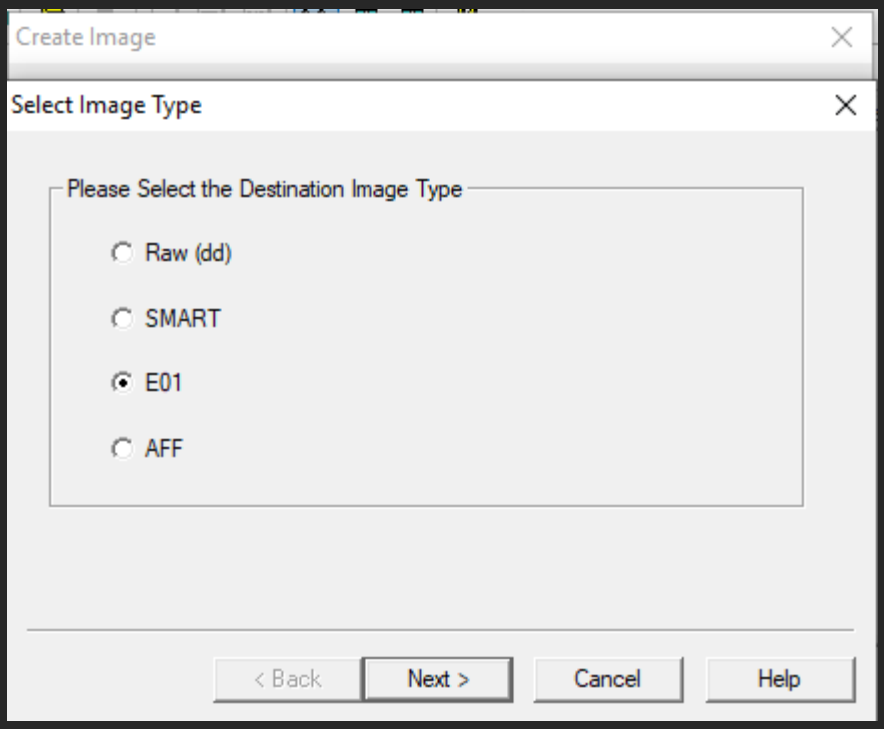

Fig. 7.

E01 image format is chosen as shown in the figure 7, just do the same and click next.

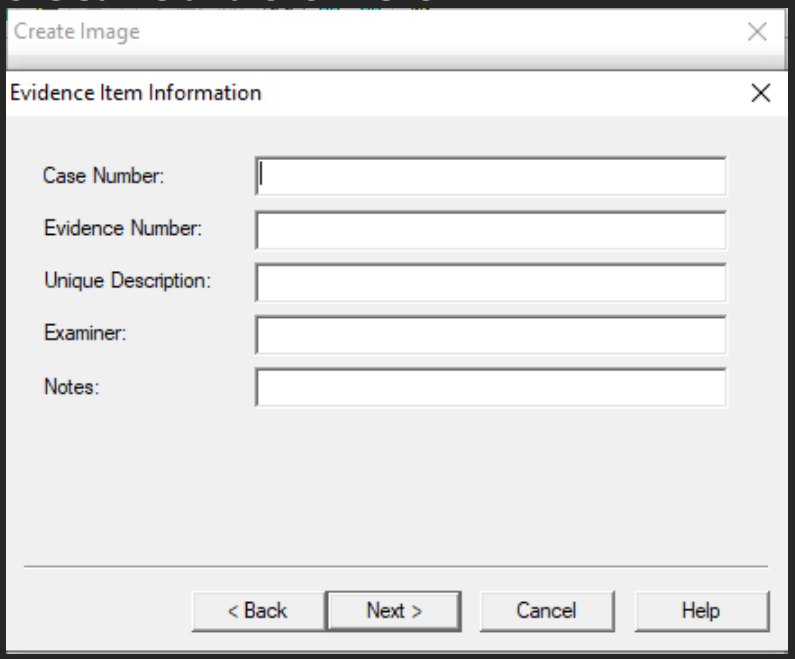

Fig. 8.

Figure 8 shows information fields to be filled, just fill them as shown in the figure 9, then click next.

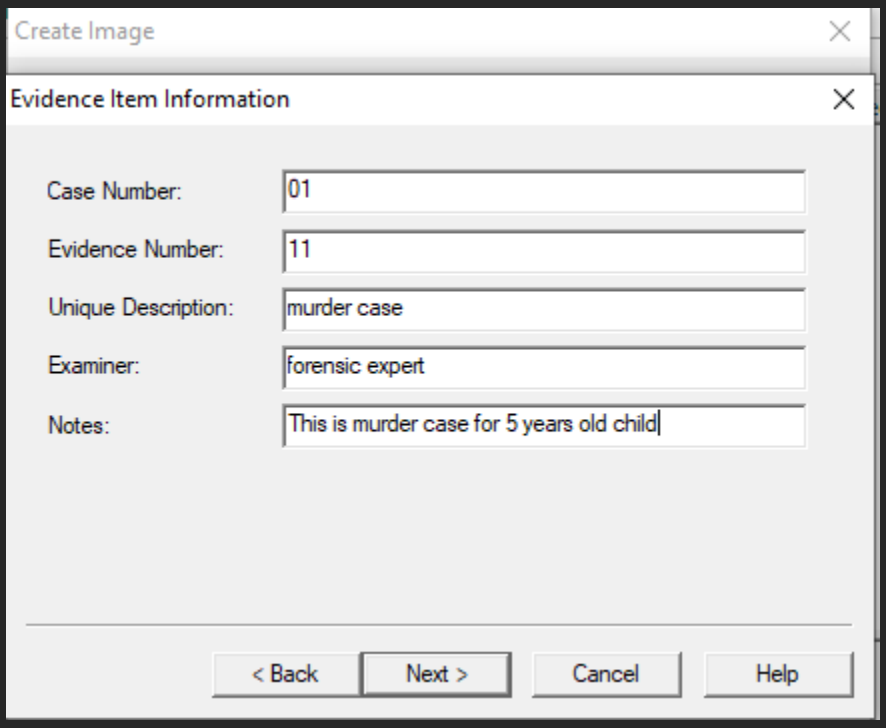

Figure 9.

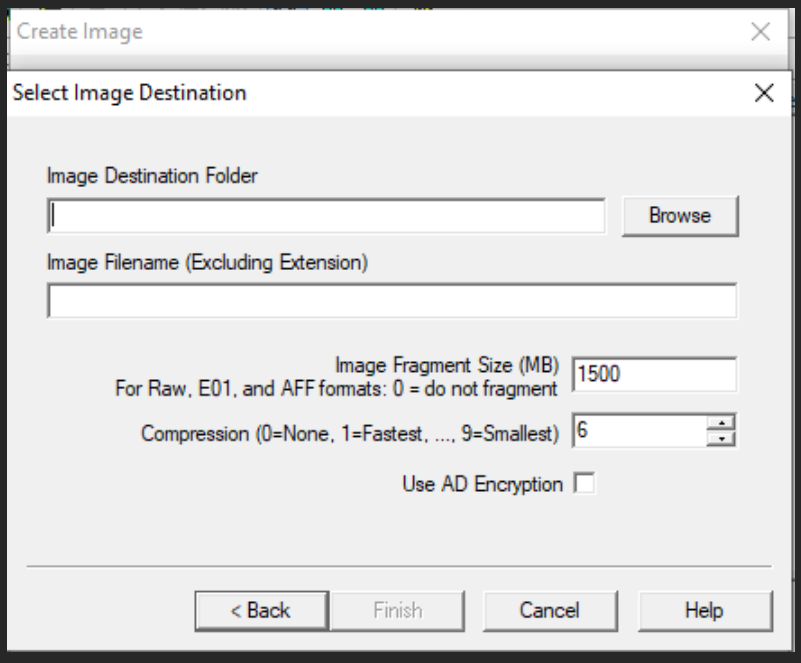

Figure 10.

If you remember Source Image is shown in the figure 6 which is USB with size of 16 GB, now it is time to choose the place where the image will be stored after being created and

underneath of Image Destination Folder is the Image Filename. Click on the browse to browse the destination file.

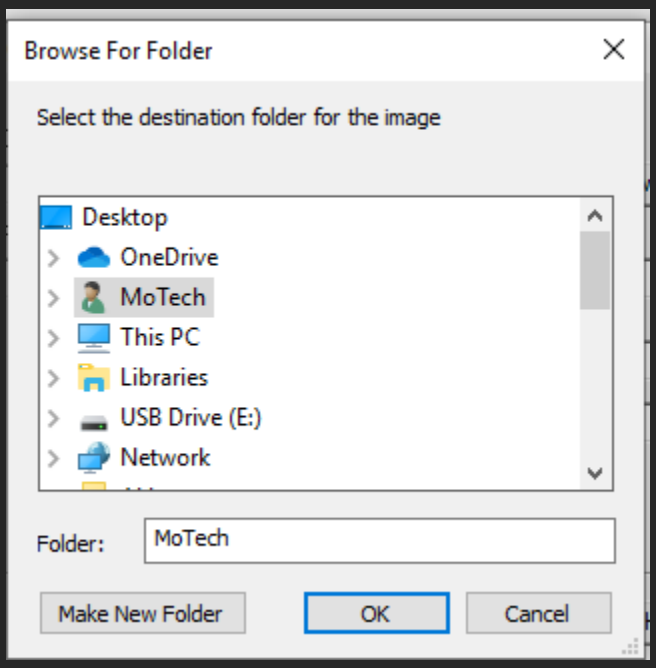

Figure 11.

At the bottom of figure 11, click on the option Make New Folder for storing image.

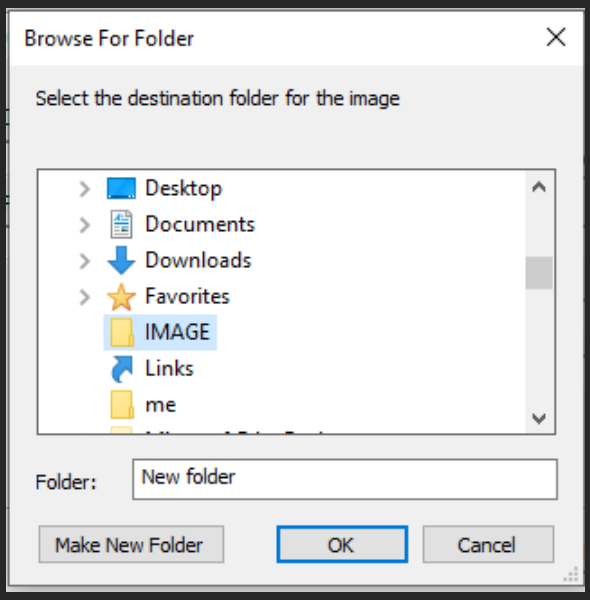

Figure 12.

On the desktop create folder called IMAGE, select it and click ok as shown in the figure 12.

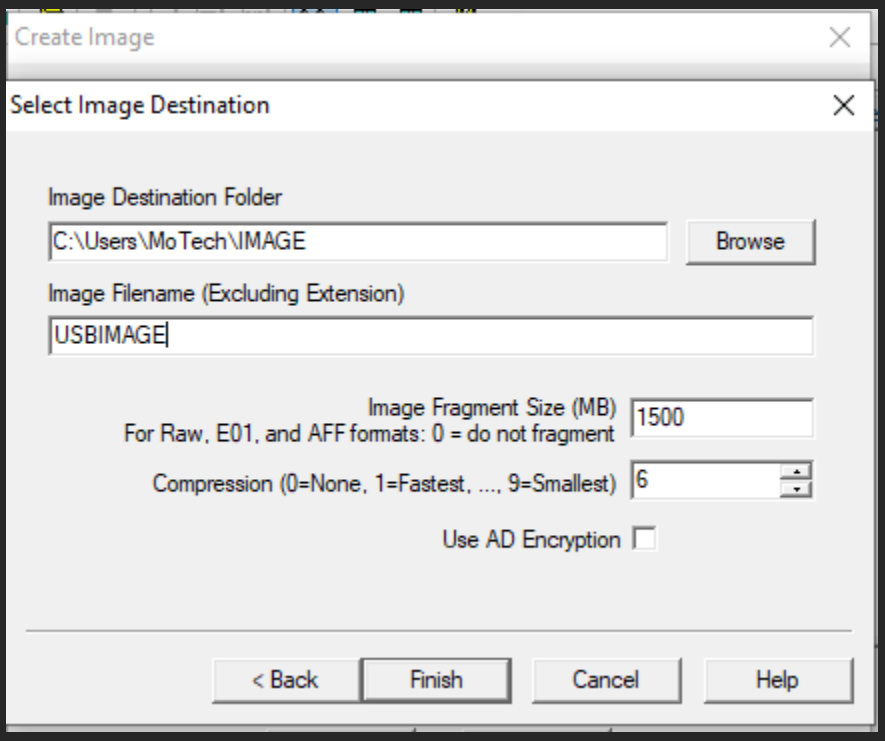

Figure 13.

Give filename USBIMAGE as shown in the figure 13, after that click finish as shown in the bottom of figure 13.

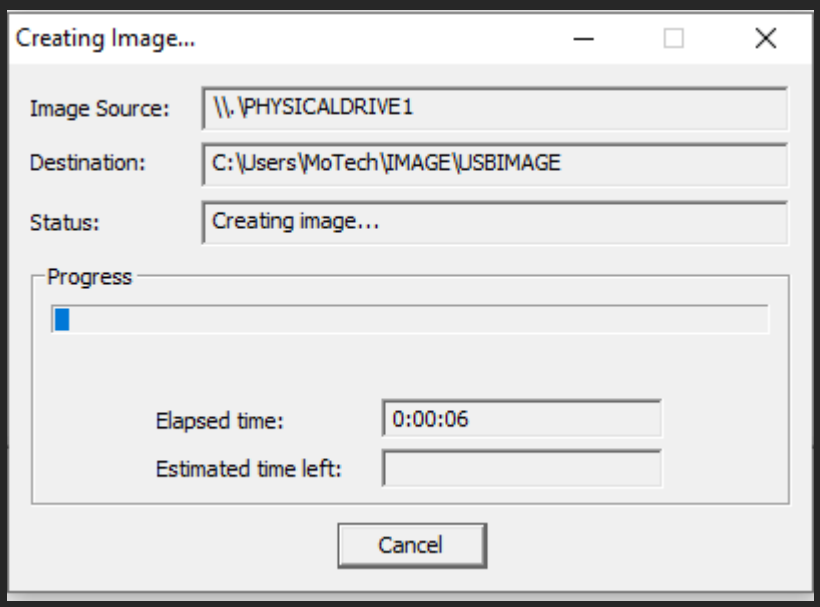

Figure 14.

After clicking finish, then click start and your application should come with new window as shown in the figure 14.

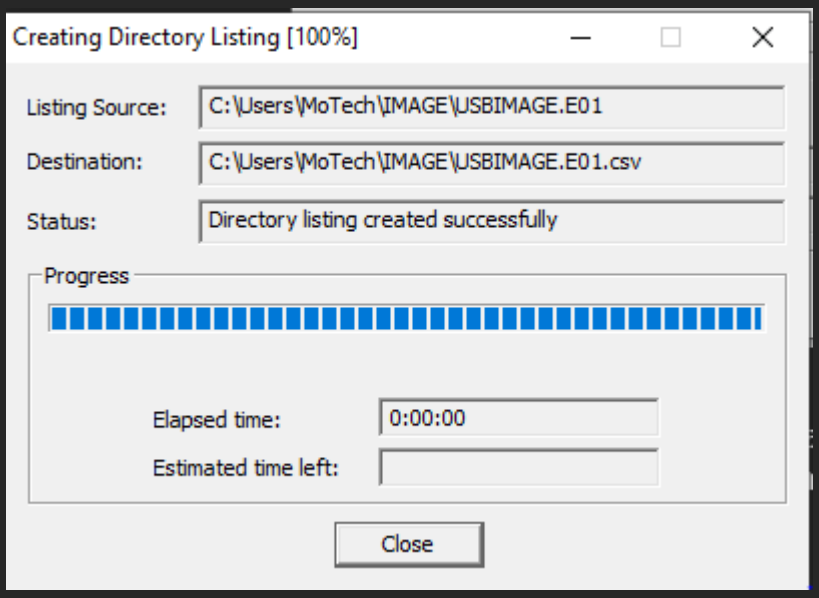

Figure 15.

Status in the figure 15 shows that image is successfully created.

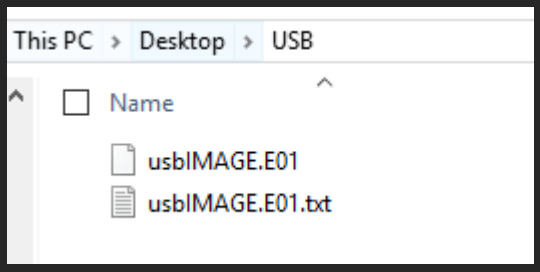

Figure 16.

In the figure 16 we can see our image of format E01 is created.

CONCLUSION.

This is the end of my article, after creating disk I hope you enjoy, more one more thing I want to tell you is that forensic is one of the biggest field, want you suppose to do is try and use different tools of forensic, also be wide, go through network forensic, device forensic, disk forensic and mobile forensic, I will try to share more of my articles on this field, without forgetting to produce YouTube videos tutorials about forensic.

Do not miss my next article on which you will learn how to make analysis of disk image created by FTK image creator.

WAYS TO GET IN TOUCH WITH MoTech.

Linkedin.com

https://www.linkedin.com/in/motech-inc-720261191/

YouTube.com

https://www.youtube.com/channel/UCtuaigKZF3okQnKON5RM1qQ

Amazon.com
https://www.amazon.com/s?k=noel+moses+mwadende&ref=nb_sb_n oss

Github.com

https://github.com/MoTechStore/

Scribd.com

https://www.scribd.com/user/470459684/MoTech

SlideShare.com

https://www.slideshare.net/MoTechInc?utm_campaign=profiletracking&utm_ medium=sssite&utm_source=ssslideview