PROTECT ALTERATION OF DATA IN USB DRIVE

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.

Data integrity is the protection of data from unauthorized modification or improper modification, if data are tampered then they are meaningless, assume you that when you deposit $100,000 at your bank account, the message is tampered as if you have deposited $10,000, how much loss you get ?, it is about $90,000 and now you can see how data integrity is very important aspect of security, here it comes the purpose of this article, is to teach you reader of this book on how you can secure any alteration or modification of data present in the USB drive, for the purpose of maintaining the integrity of the device and data present inside it.

In forensic this concept is also used, when doing device forensic it is important is protect the alteration of data present in device. Digital forensic and integrity are the two forces drove me to write this article.

Plugin your USB drive in the port of computer, then at the search bar type CMD and make sure that command prompt come up as shown in the figure 1.

NOTE: Remember that command prompt is case insensitive, so you can type your commands by using small or capital letter, it is the matter of your choice.

STEP 1. Diskpart.

On the command prompt type diskpart and make sure that, your output looks similar with that shown in the figure 1.

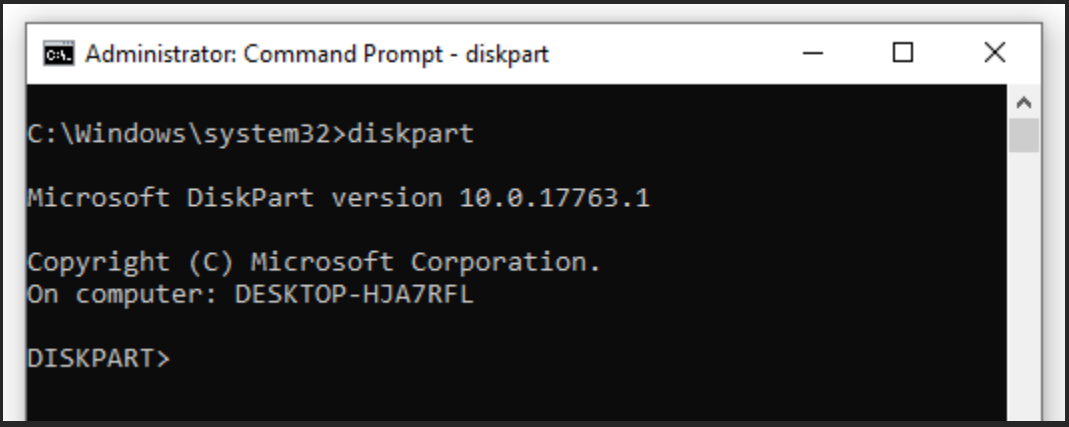

Fig. 1.

According to techopedia.com, diskpart is the manually utility with a command line that allows users to alter a disk, drive, partition or volume. The meaning of command from techopedia.com is quite true, as we are going to alter the properties of the USB drive from read and write permission to readonly permission.

STEP 2. List disk.

This command will detect all hard drives in the computer and list them, as shown in the figure 2, where by USB drive and 1TB hard disk are detected and listed down.

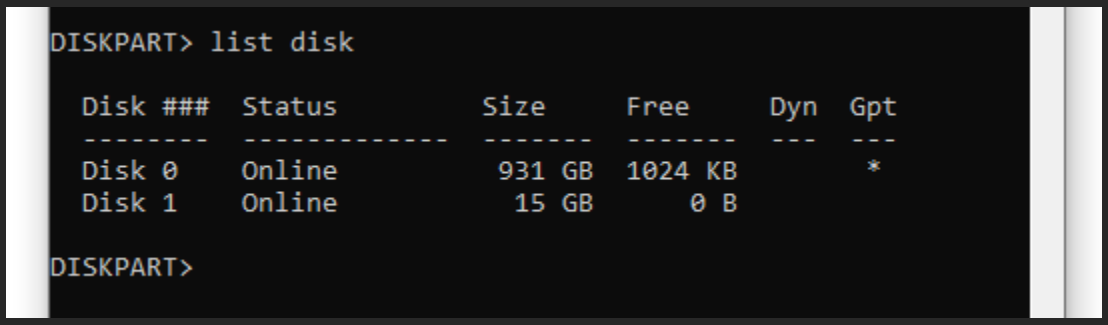

Fig. 2.

STEP 3. select disk 1.

Command is easily understood, select command is used for choosing which disk should be put in the use, I mean current working hard drive which is Disk 1.

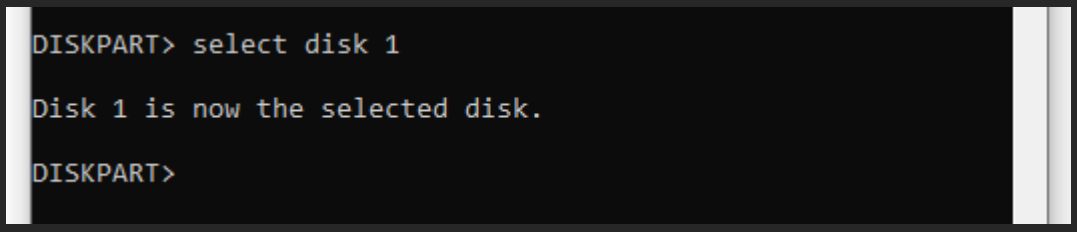

Fig. 3.

STEP 4. attributes disk.

Command attributes disk is used to check attributes of the selected drive, which is Disk 1. It is very important to check current property of the disk before alteration of the permission.

```
DISKPART> attributes disk
Current Read-only State : No
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No
```

Fig. 4.

As it is shown in the figure 4, state of USB drive is in not in the readonly, so we are going to change the permission to write and make USB drive as readonly.

STEP 5. attribute disk set readonly.

Command above will set USB drive into readonly state and protect user from writing it, this will ensure data integrity present in the USB drive.

```
DISKPART> attributes disk set readonly

Disk attributes set successfully.

DISKPART>
```

Fig. 5.

As shown in the figure 4, USB is mode in readonly state which will protect any user from making modification.

STEP 6. Attribute disk clear readonly.

If you want to remove readonly state of your USB drive after completing the task of data protection from modification, use above command and USB drive will back to it's normal condition.

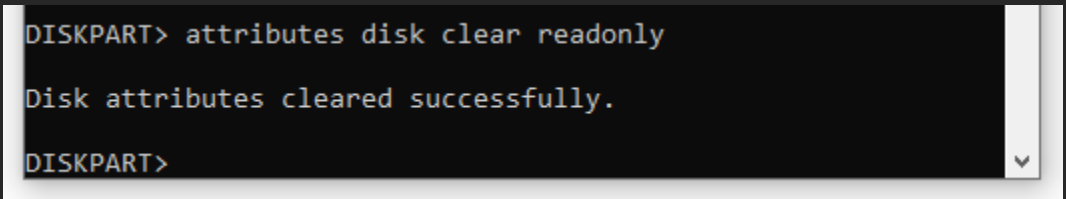

Fig. 6.

CONCLUSION.

That is the end of this article, make sure you follow command written and shown in the figures, data is valuable if it is protected, ensure you keep your data in secure state, permission and properties, thank you.

After protecting this device from being altered, the next thing to do is to create disk image by using FTK image creator, so do not miss my next articles, it will be like a series of forensic article series.

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