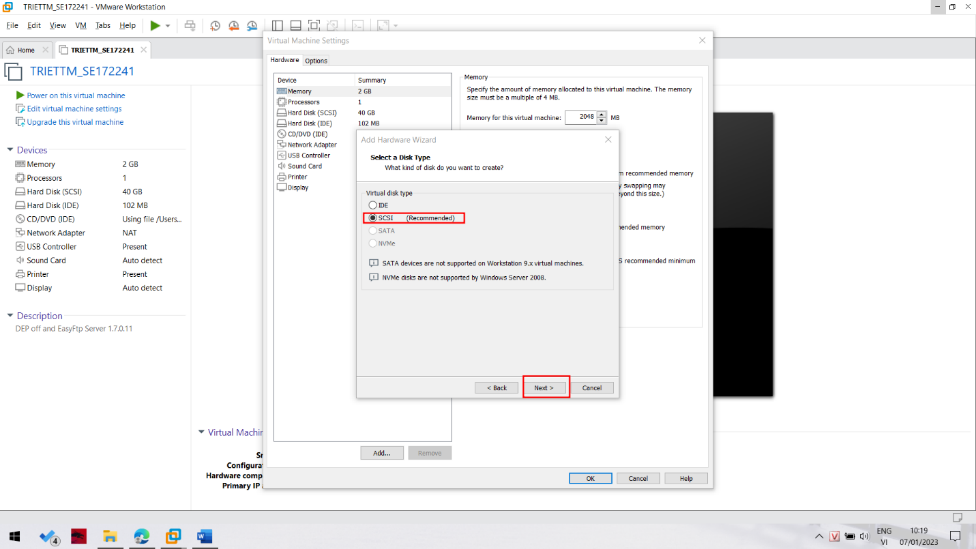
**Lab 11: Using FTK**

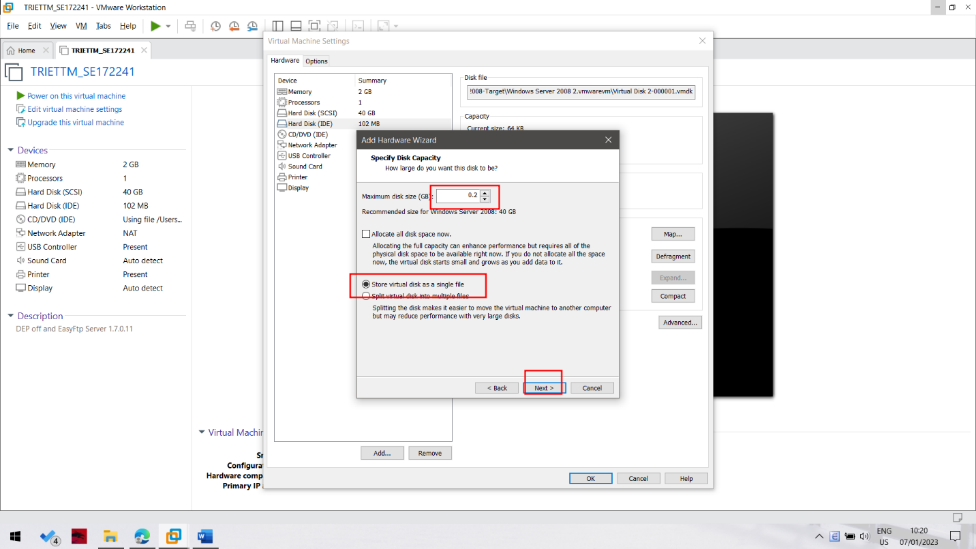
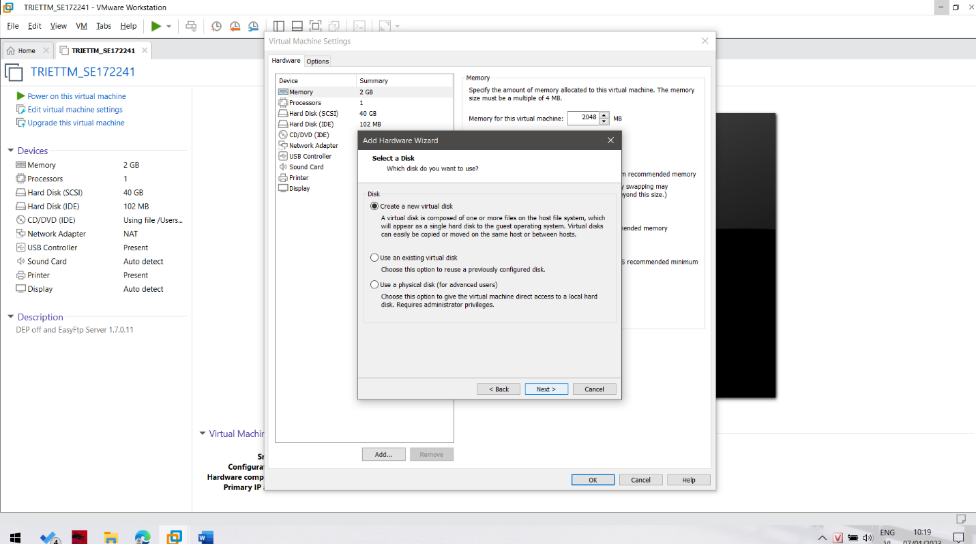
Making a Clean Disk

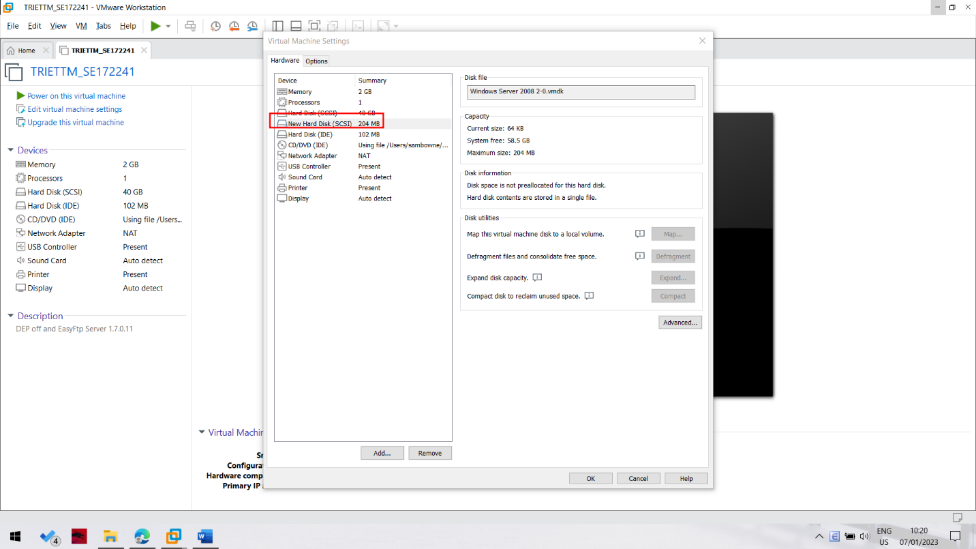
You should have a small virtual hard drive attached to your VM, which you created in a previous project. If you don't have one, create one now, or plug in a USB flash drive. It doesn't matter what data is on it for now

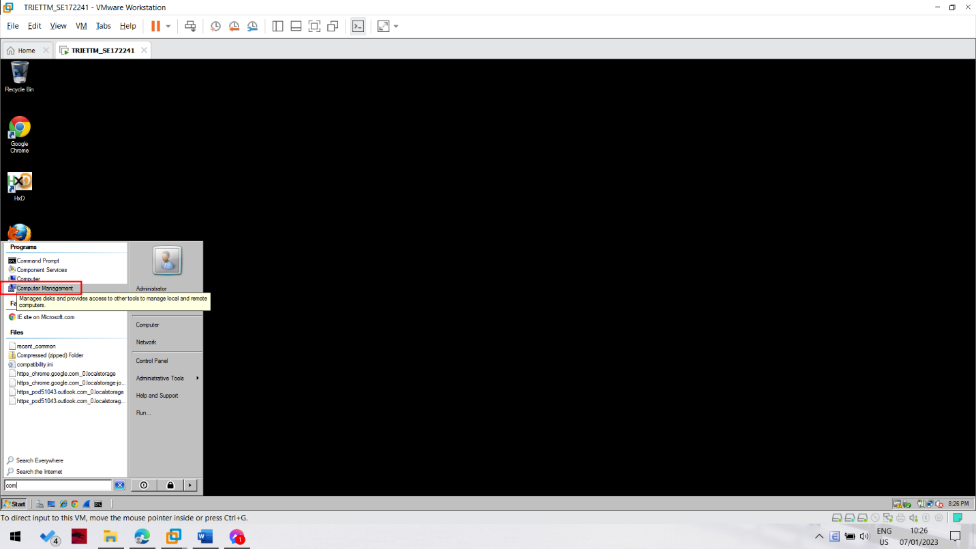
Click Start, right-click "My Computer", and click Manage.

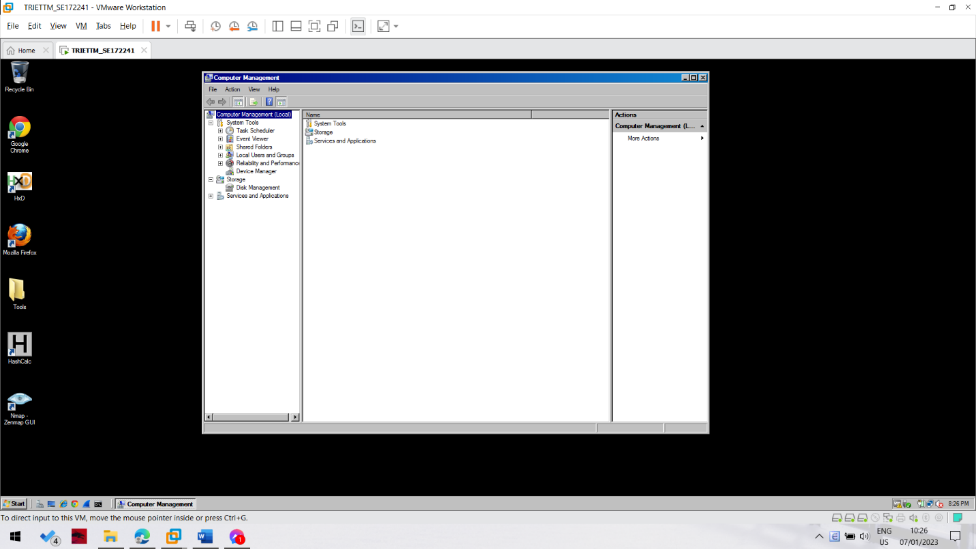
You should see your second small disk labelled "Disk 1", as shown, e.g. below.

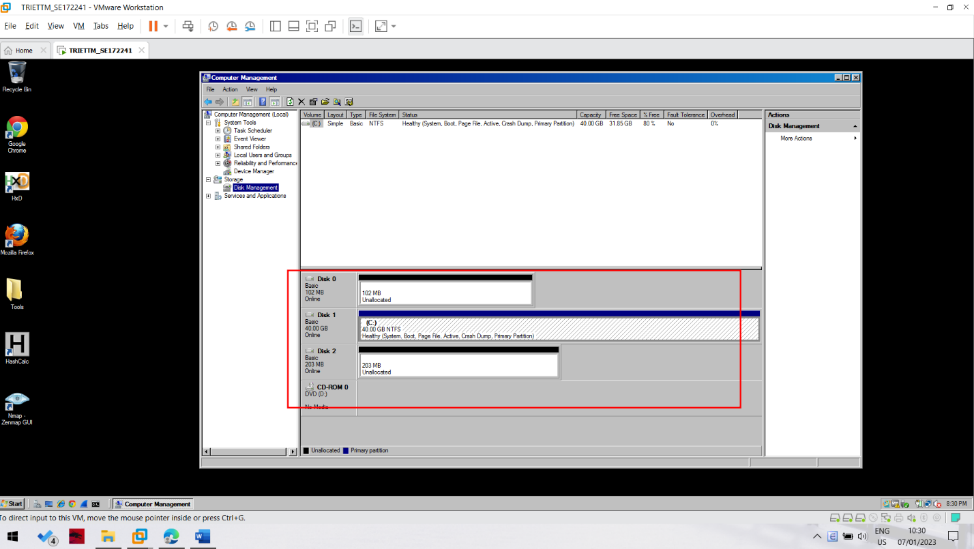












Click Start, Run. Type CMD and press Enter.

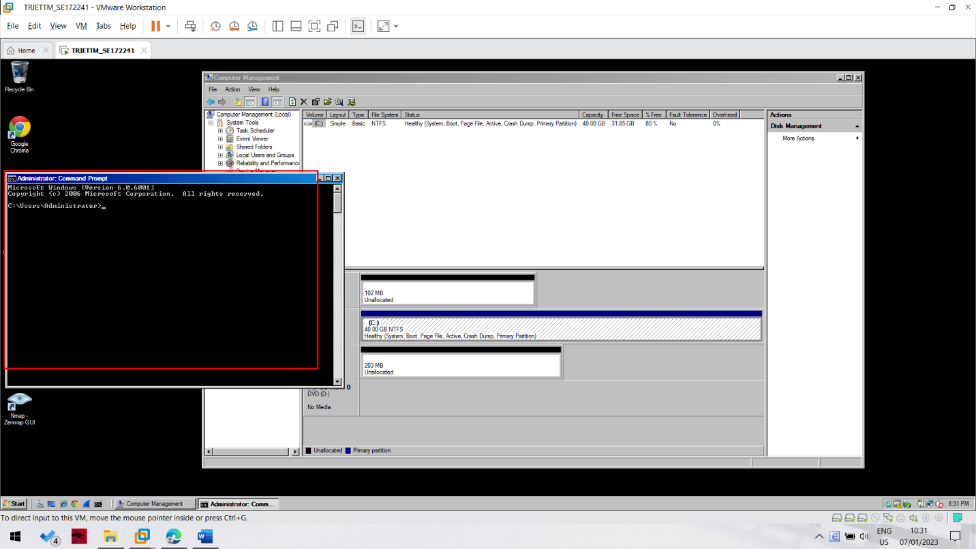
Execute these commands to clean your second disk. Be careful not to erase the wrong disk!

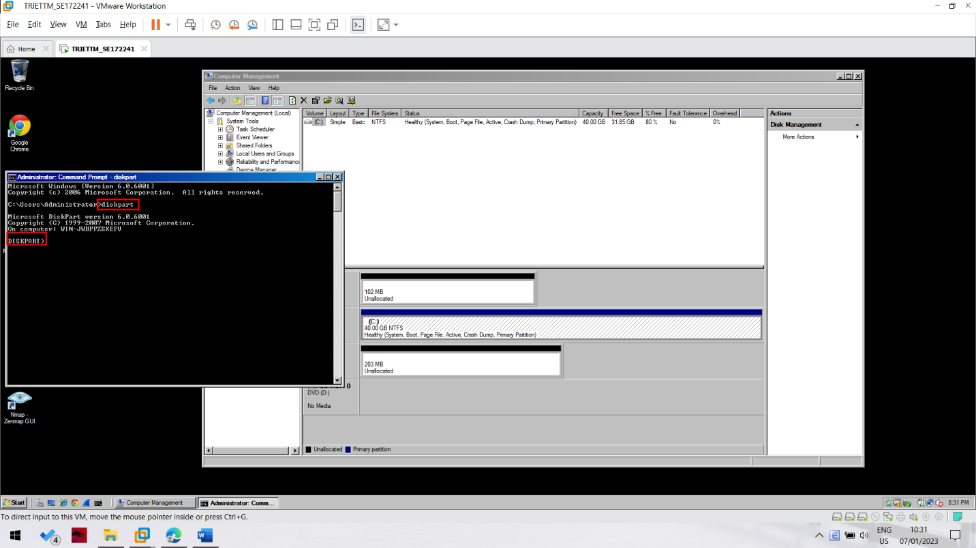
DISKPART

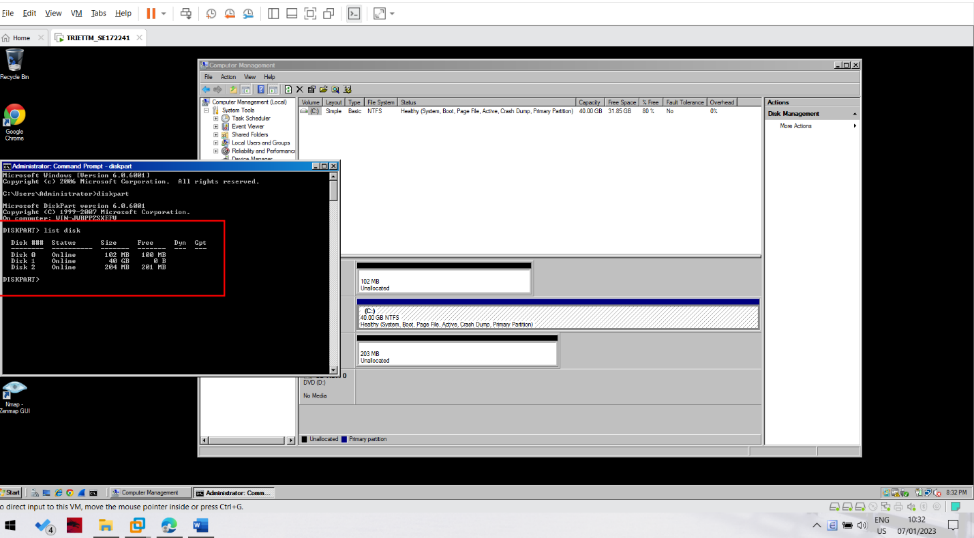
LIST DISK

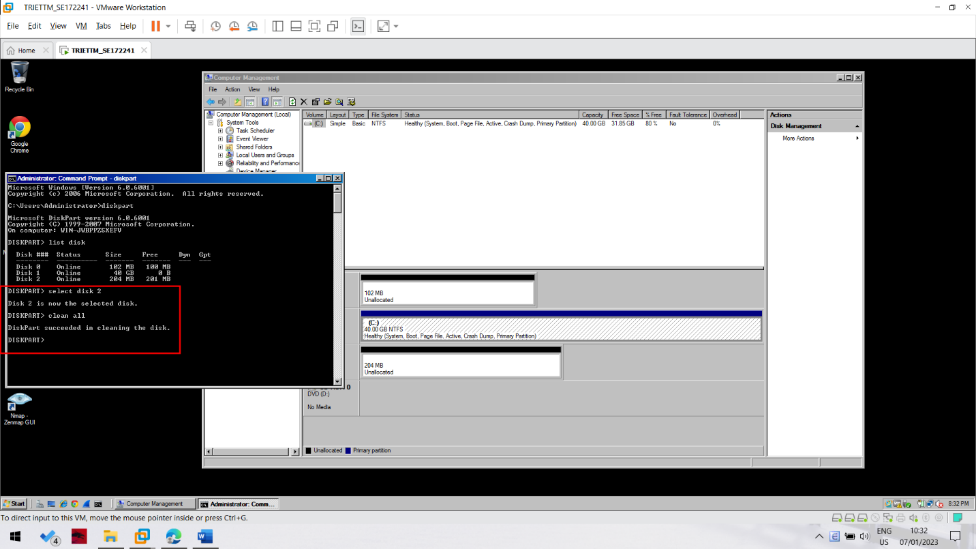
SELECT DISK 1

CLEAN ALL

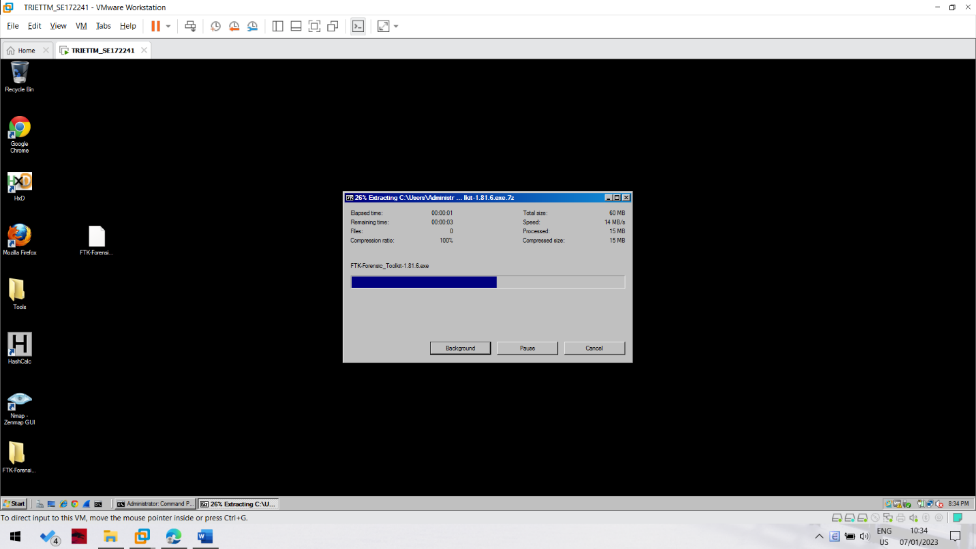


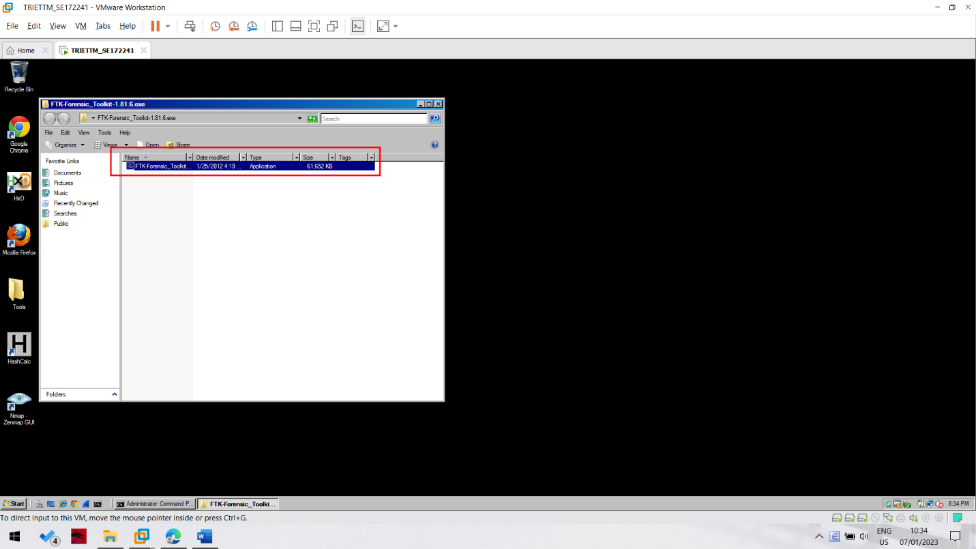


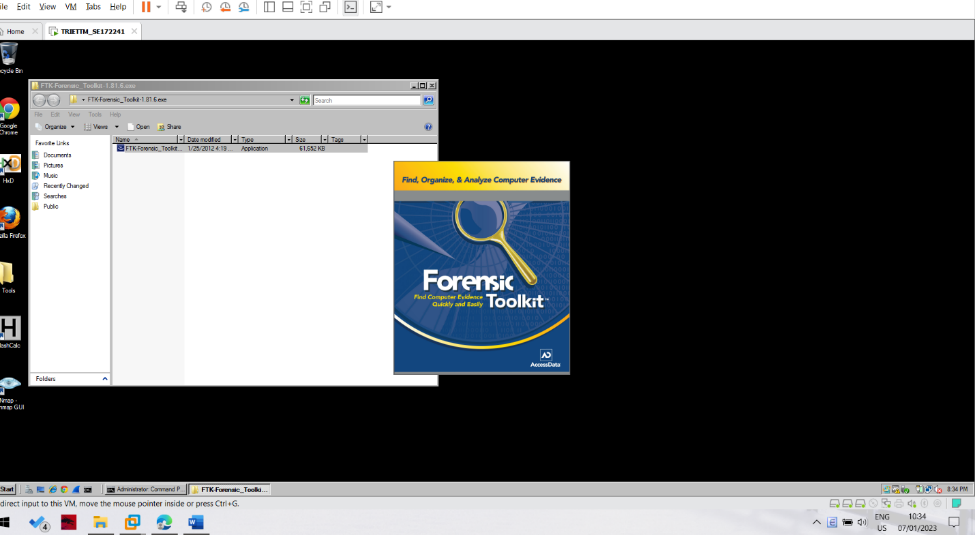


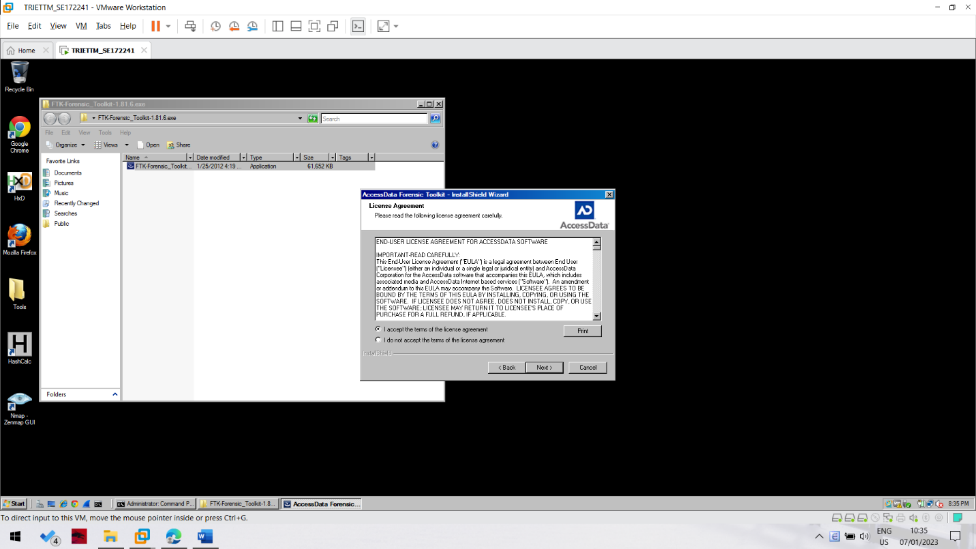


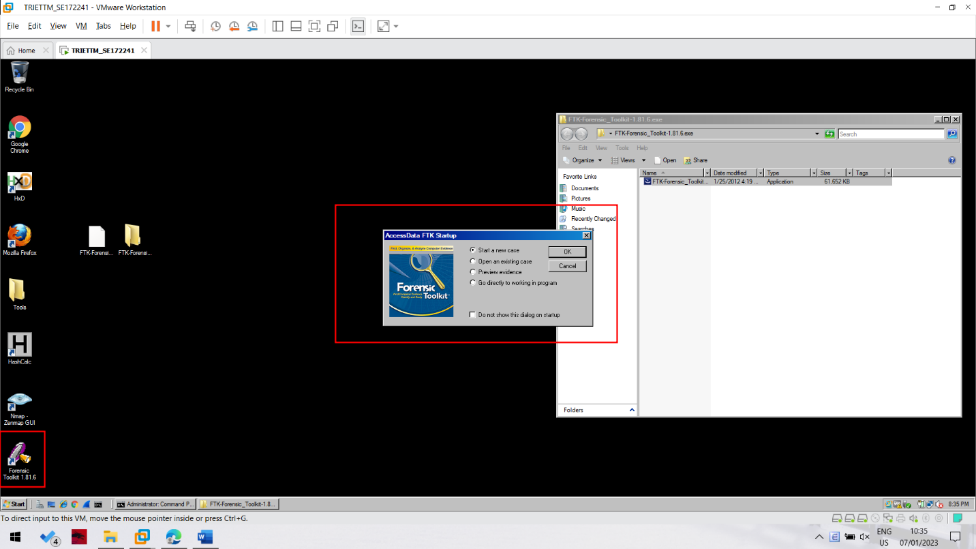
Downloading FTK

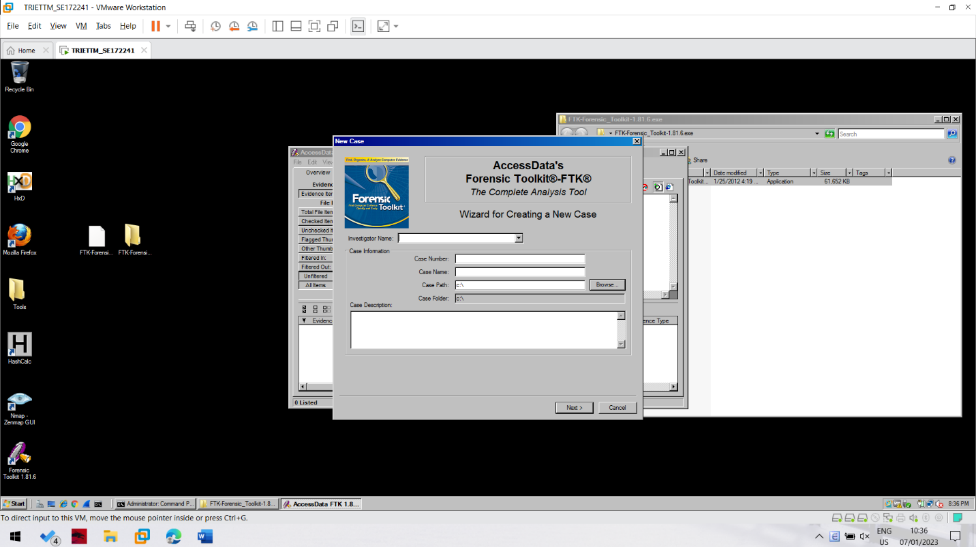


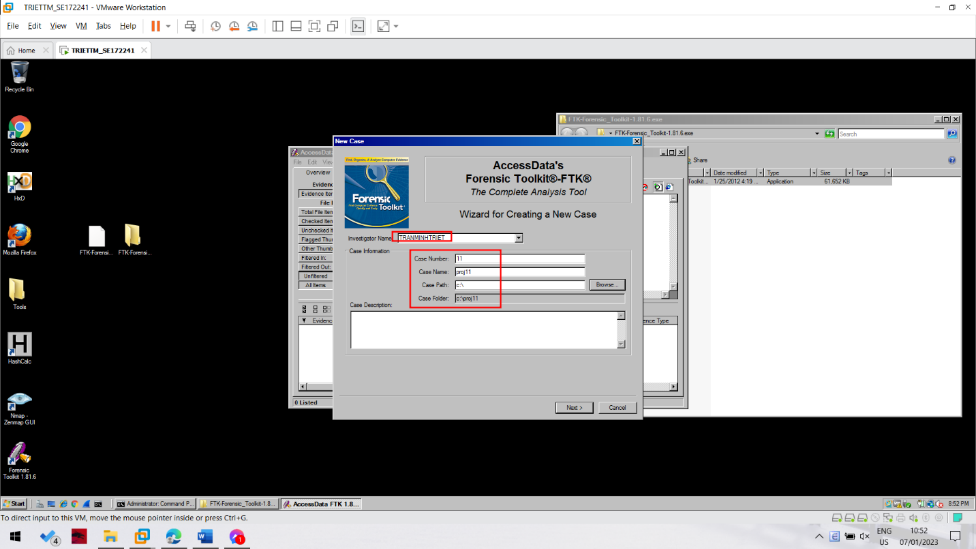








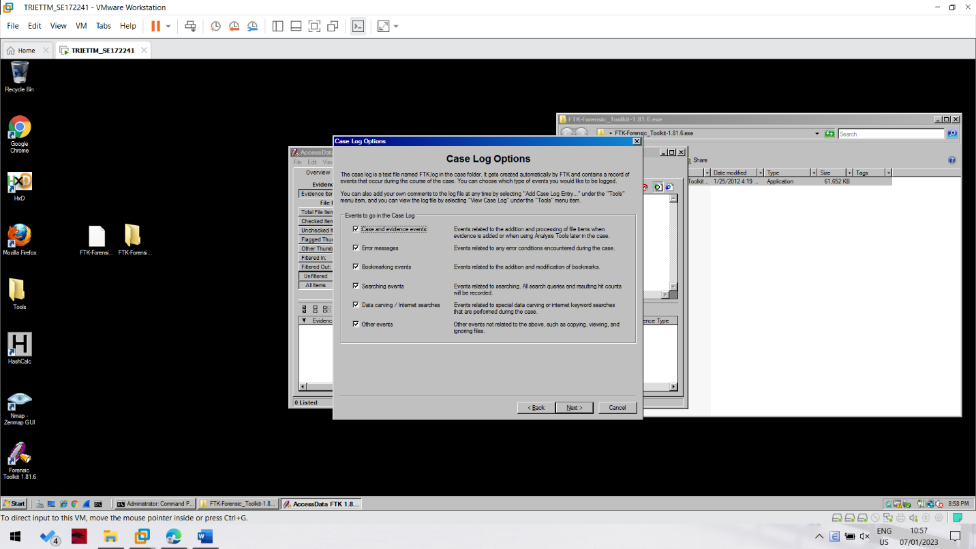




In the screen titled "Forensic Examiner Information", leave the fields blank and click Next.

In the screen titled "Case Log Options", accept the default selections, which will log everything. Click Next.

In the screen titled "Processes to Perform", deselect "KFF Lookup" and "Decrypt EFS Files", because those features won't work in the demo version, as shown below. Click Next.

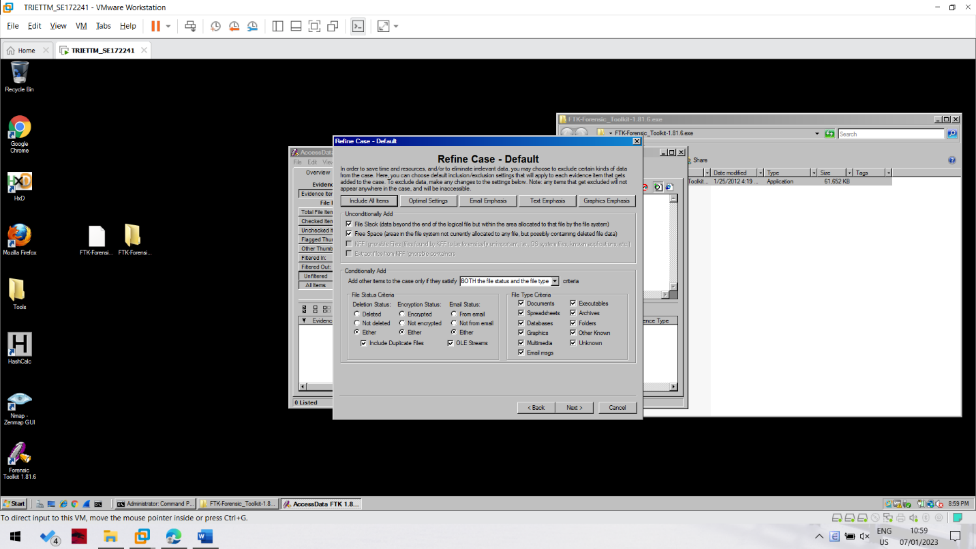


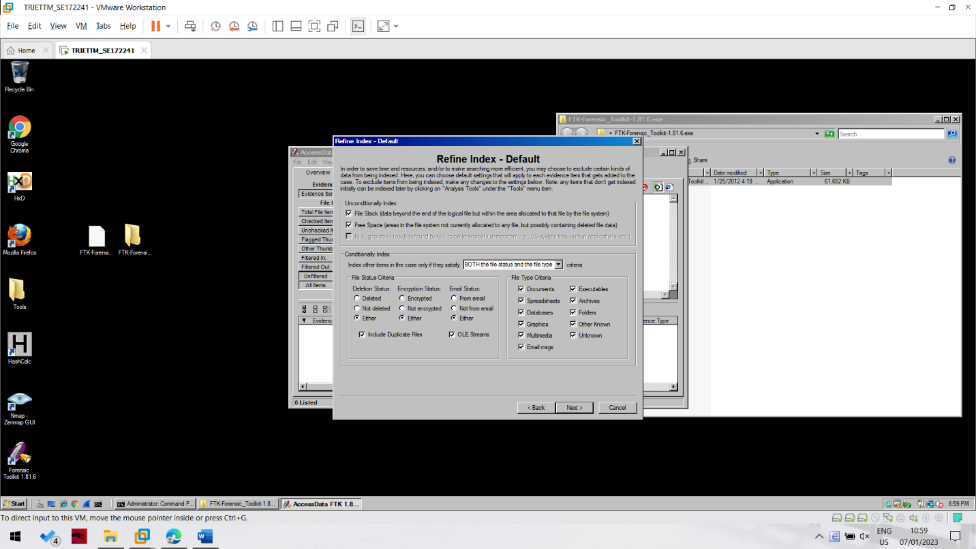


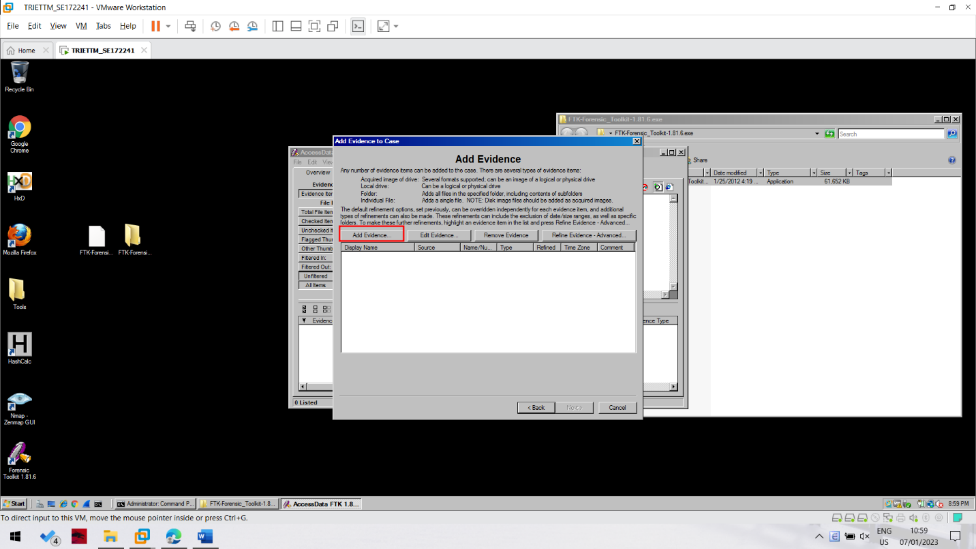
In the screen titled "Refine Case-Default", accept the default of "Include All Items". Click Next.

In the screen titled "Refine Index -Default", accept the default options. Click Next.

Now you see the "Add Evidence" screen, as shown below.





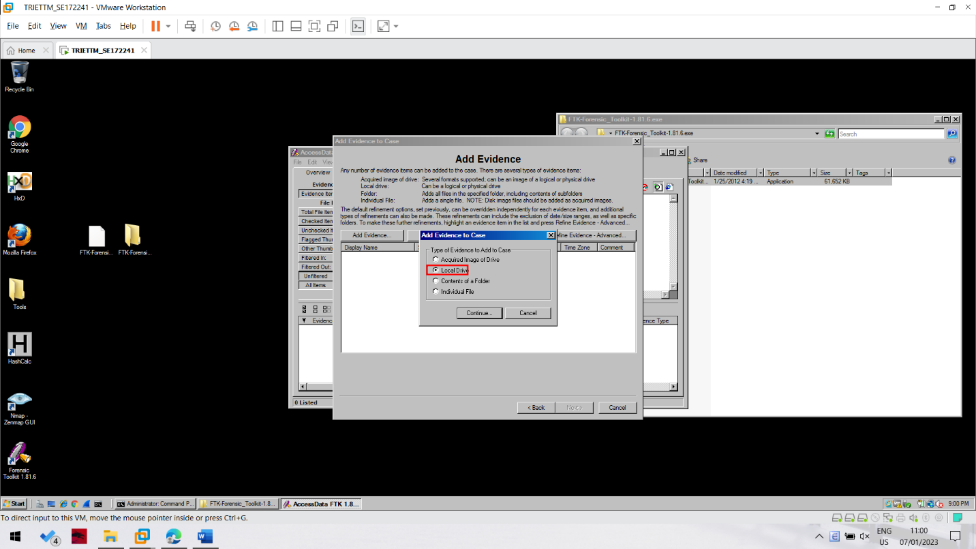


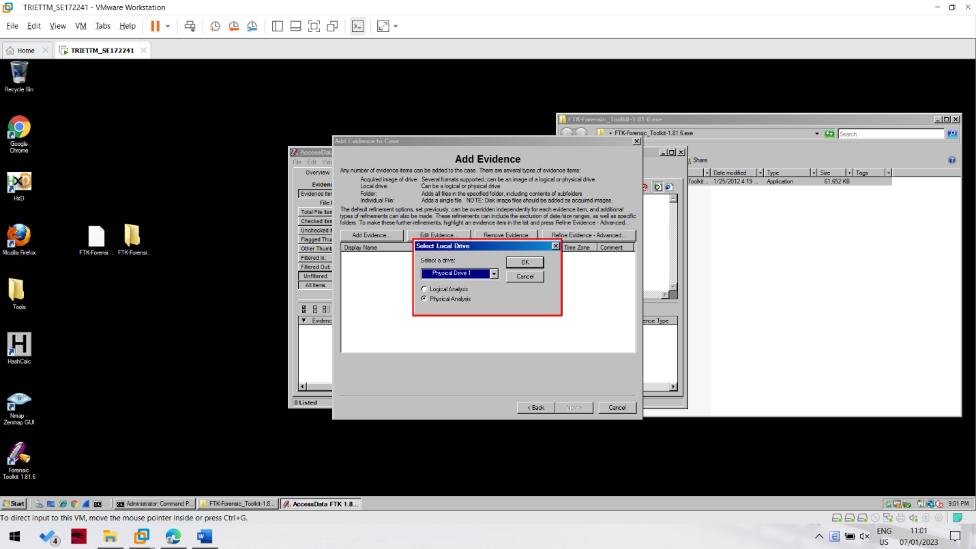
Adding Evidence to the Case

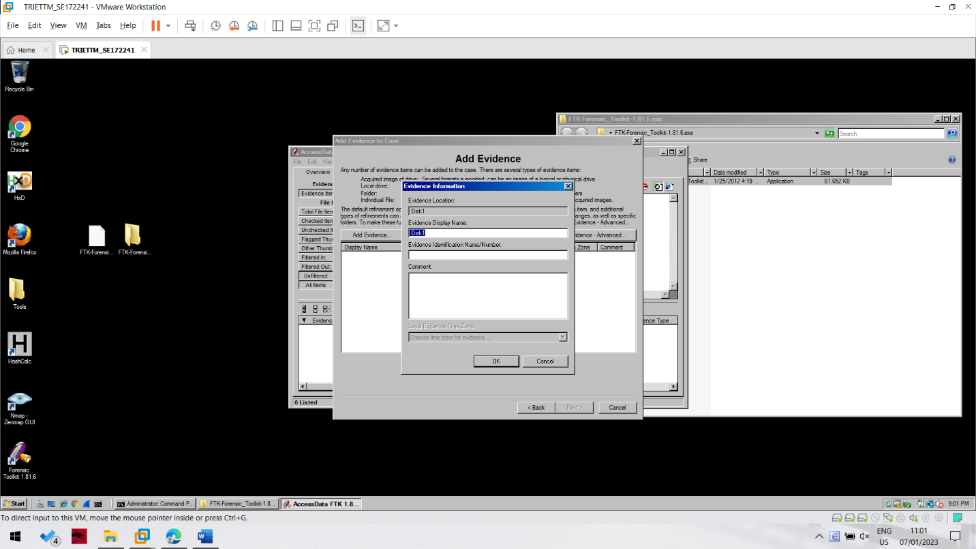
In the "Add Evidence" box, click the "Add Evidence...". button.

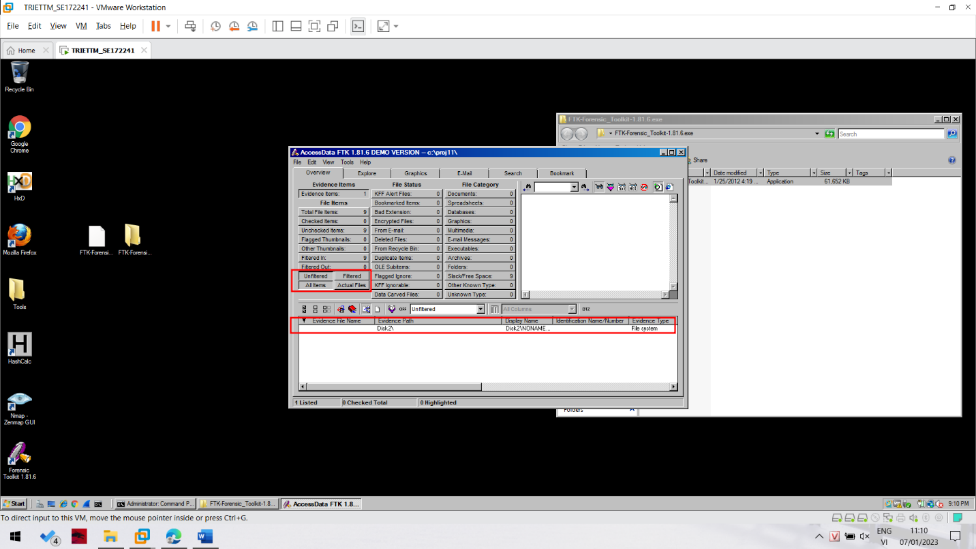
In the "Add Evidence to Case" box, select "Local Drive", and click Continue.

In the "Select Local Drive" box, click "Physical Analysis" and select the drive "Physical Drive 1", as shown below. Click OK.

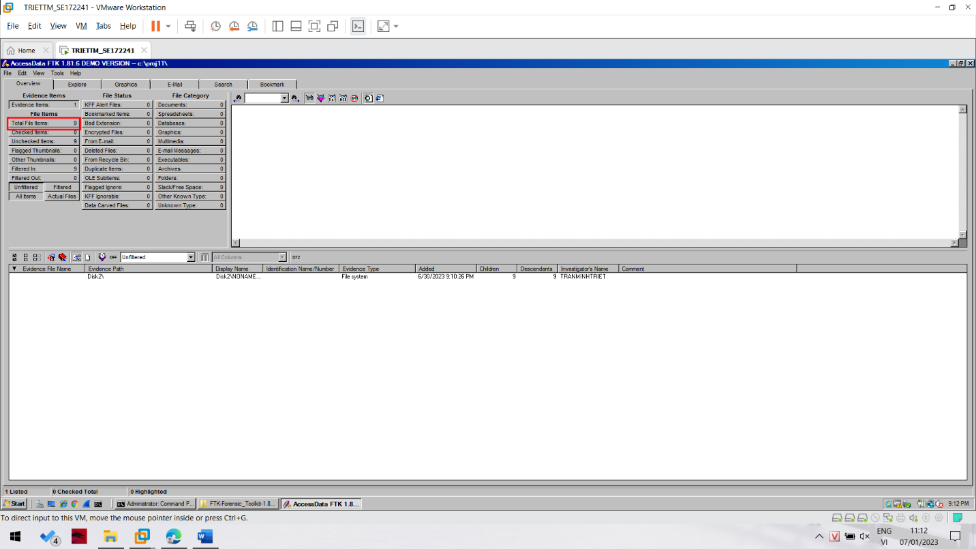






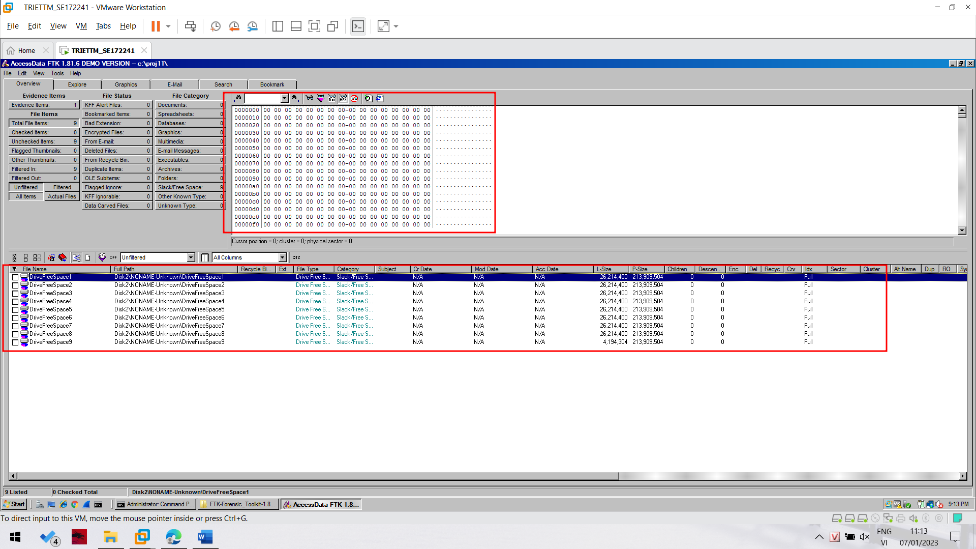


The FTK Window



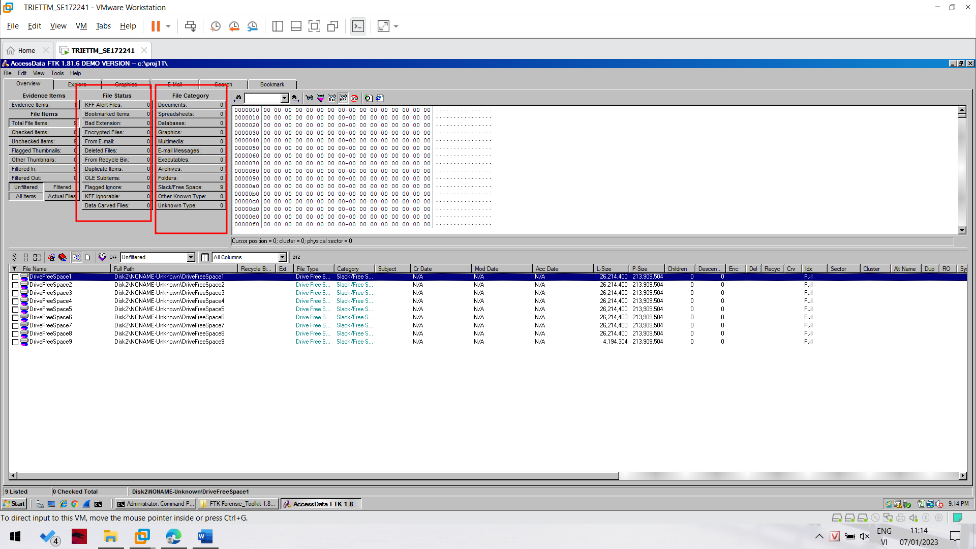
To find out, click the "Total File Items:" button. The lower pane now shows five items, named "DriveFreeSpace1","DriveFreeSpace2","DriveFreeSpace3", etc.

In the bottom pane of the FTK window, click "DriveFreeSpace1". The upper right corner now shows a hexadecimal view of the bytes in that file, as shown below.



This is just like the HxD utility you used in a previous project. As you can see, the file is empty--it's not really a file at all, because it has no header or footer or file name or any data at all. FTK just breaks empty space up into chunks it calls 'Files" for handling.

To see that the disk is really empty, look at the "File Status" and "File Category" columns in the upper left portion of the FTK window. You can see that FTK was unable to find any usable data in any known format on this disk--it's clean.



Downloading the Evidence File

