Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Ishan Aakash Patel	146151238	As Posted	6%

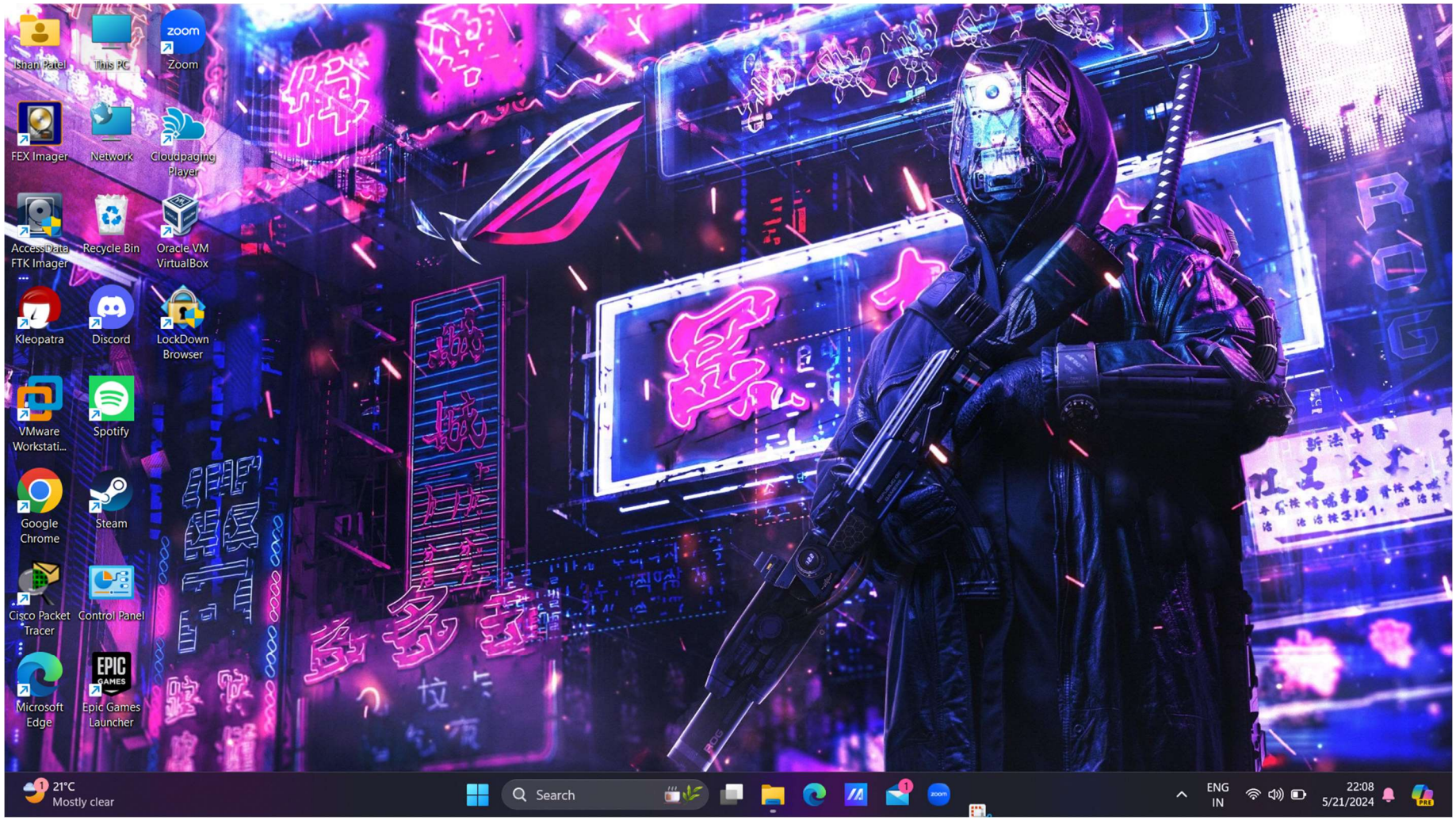
Name	Lab1: Create Image File for Disk

Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above.
	• Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
	• Attach the main screenshots of your work performed and write your own analysis & findings of your activities.
	• Include Links & References, if applicable
	• Show your genuine signs of your work is done on your machine. This includes:
	  ○ Screenshots that show your desktop background with Date/Time
	  ○ Show a pop-up bx that shows "your name + IP".
	  ○ Show your logged account when applicable.
	  ○ Optional: Your photo.
	• Submit your report name: CYT215-Lab1-Student Name & ID

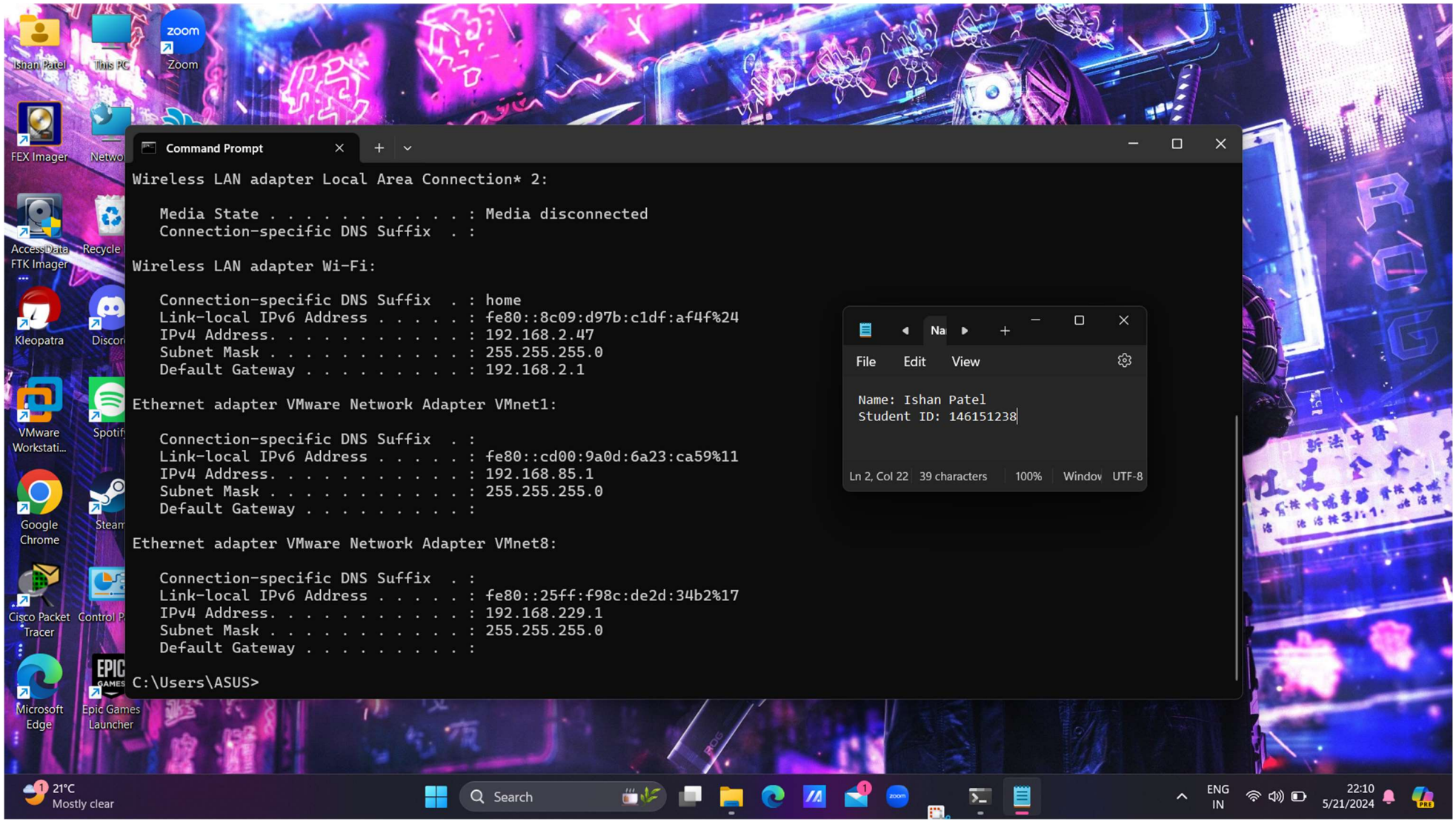
Students Work required for this activity	• Go to Read https://www.hackingarticles.in/multiple-ways-to-create-image-file-for-forensics-investigation/. You will see that there are 4 popular relevant tools:
	  1. FTK Imager
	  2. Belkasoft Acquisition Tool
	  3. Encase Imager
	  4. Forensic Imager
	• Download & install any 2 tools (upon your wish) for example the following 2 tools:
	  1. FTK Imager https://www.exterro.com/ftk-imager
	  2. Forensic imager https://getdataforensics.com/product/fex-imager/
	• Make disk image of your machine using your chosen 2 tools, i.e. A disk image for every tool (The image is typically mounted by or 'loaded into' forensics software, such as FTK Imager, for analysis which usually involves searching various areas on the disk for evidence of malicious activity or presence of malware.)
	• Take screenshots of your works.
	• Keep your images for future coming labs.
	• Briefly write your experience and answer the following.:
	  ○ Which tool you found is good & easy to use?
	  ○ How to verify that your image is correct?

Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.

Desktop Background

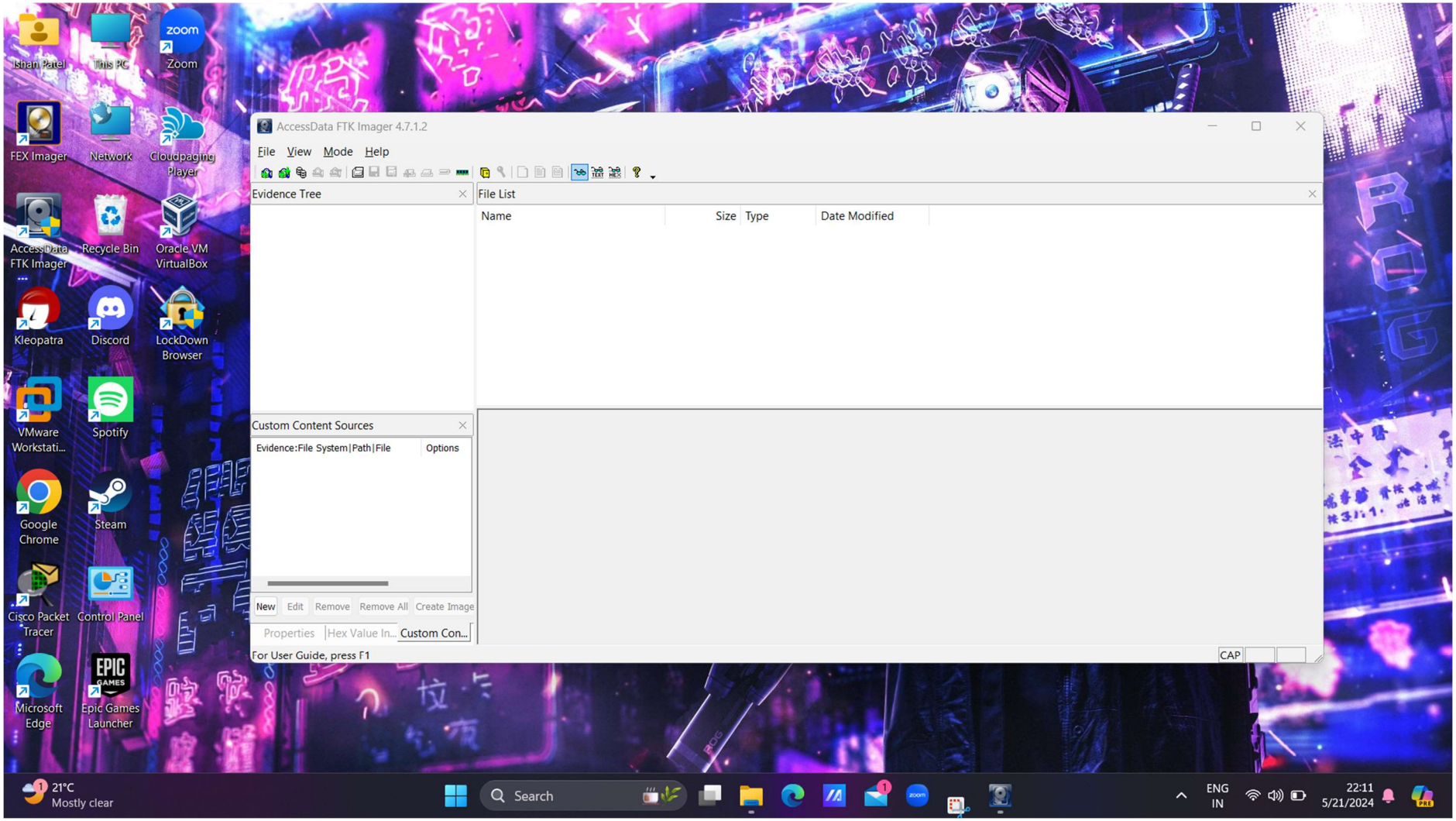


IP address and Name

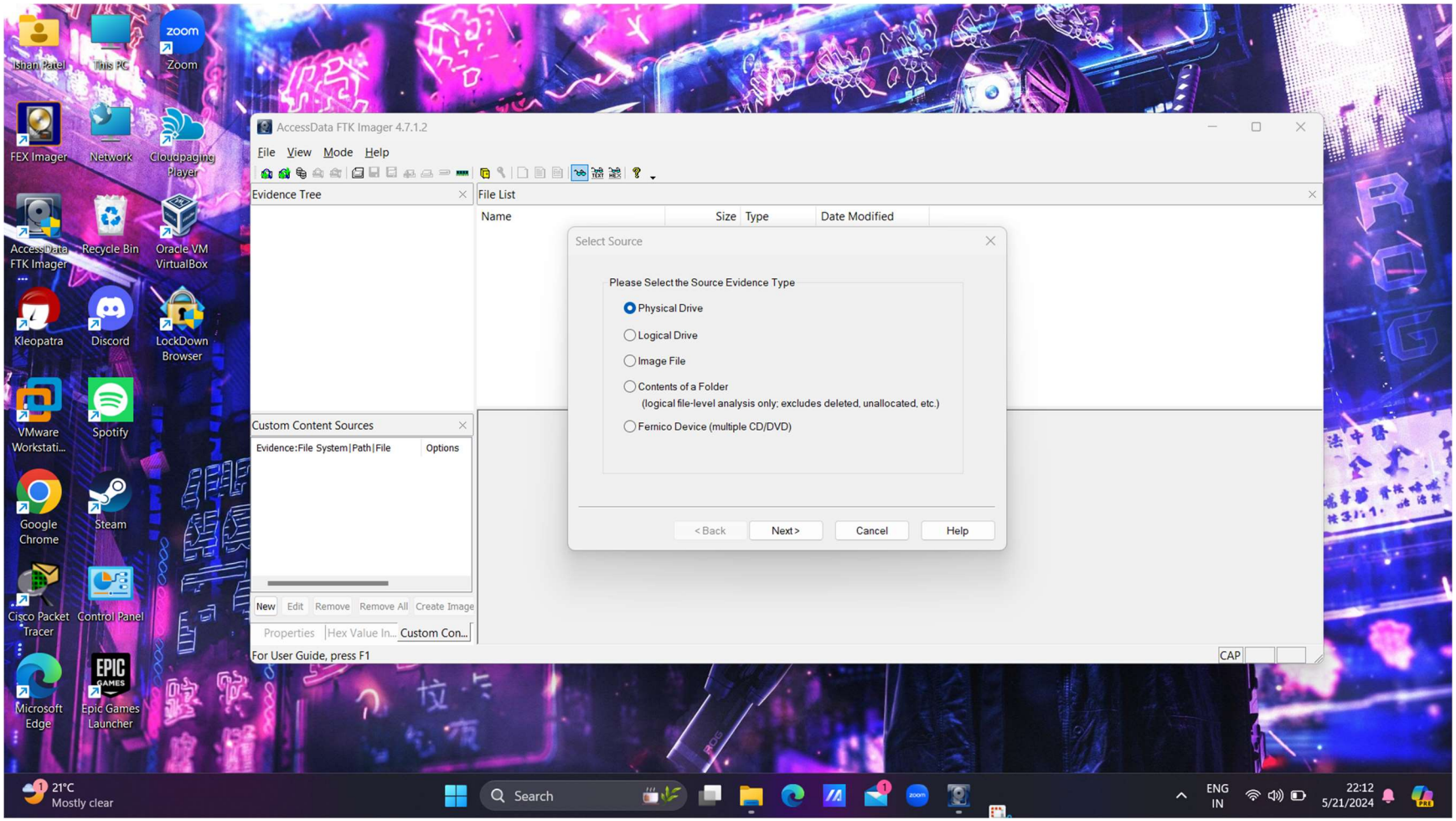


Tool 1 – FTK Imager

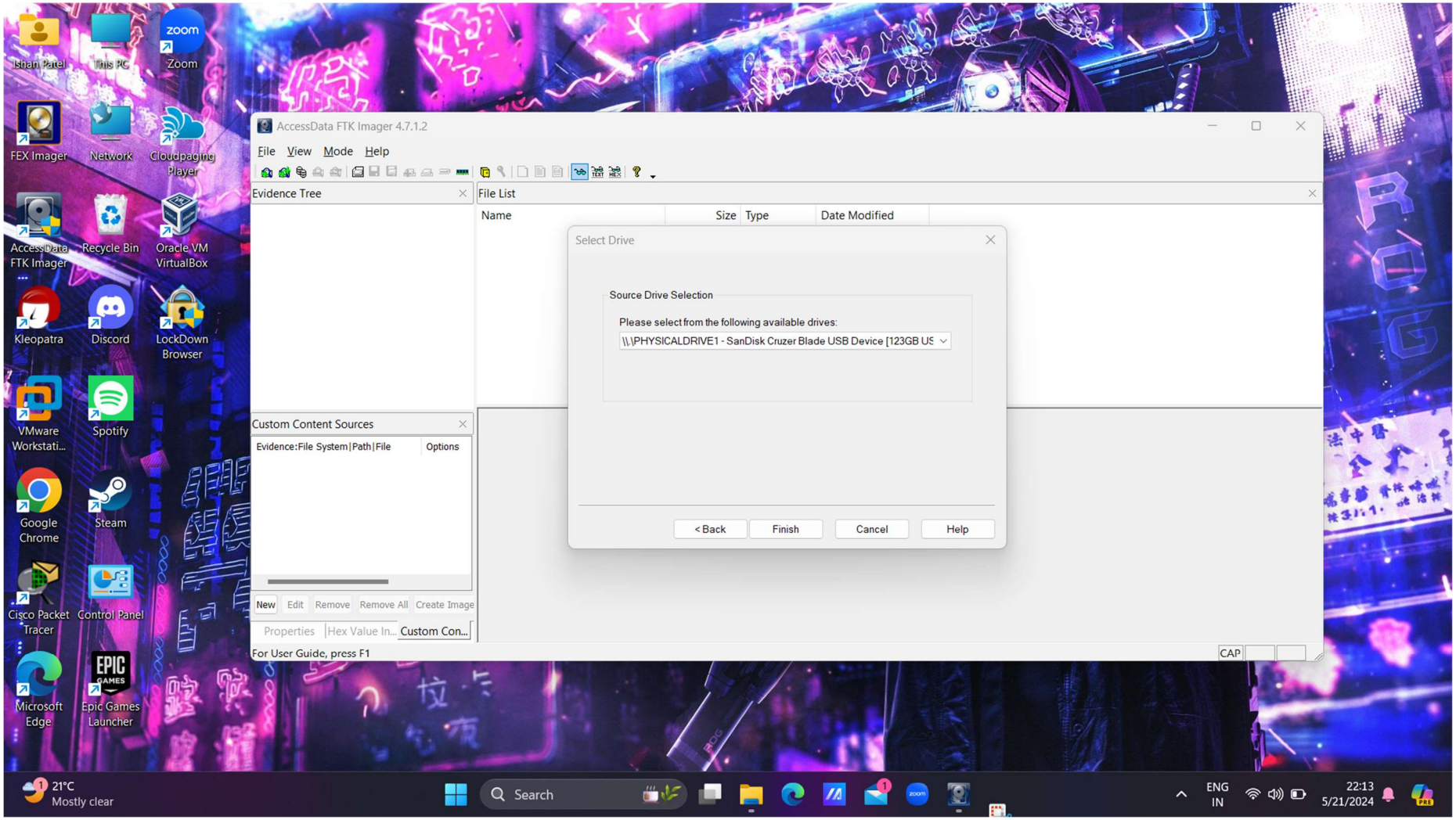
I installed the tool using the link given in the lab description.

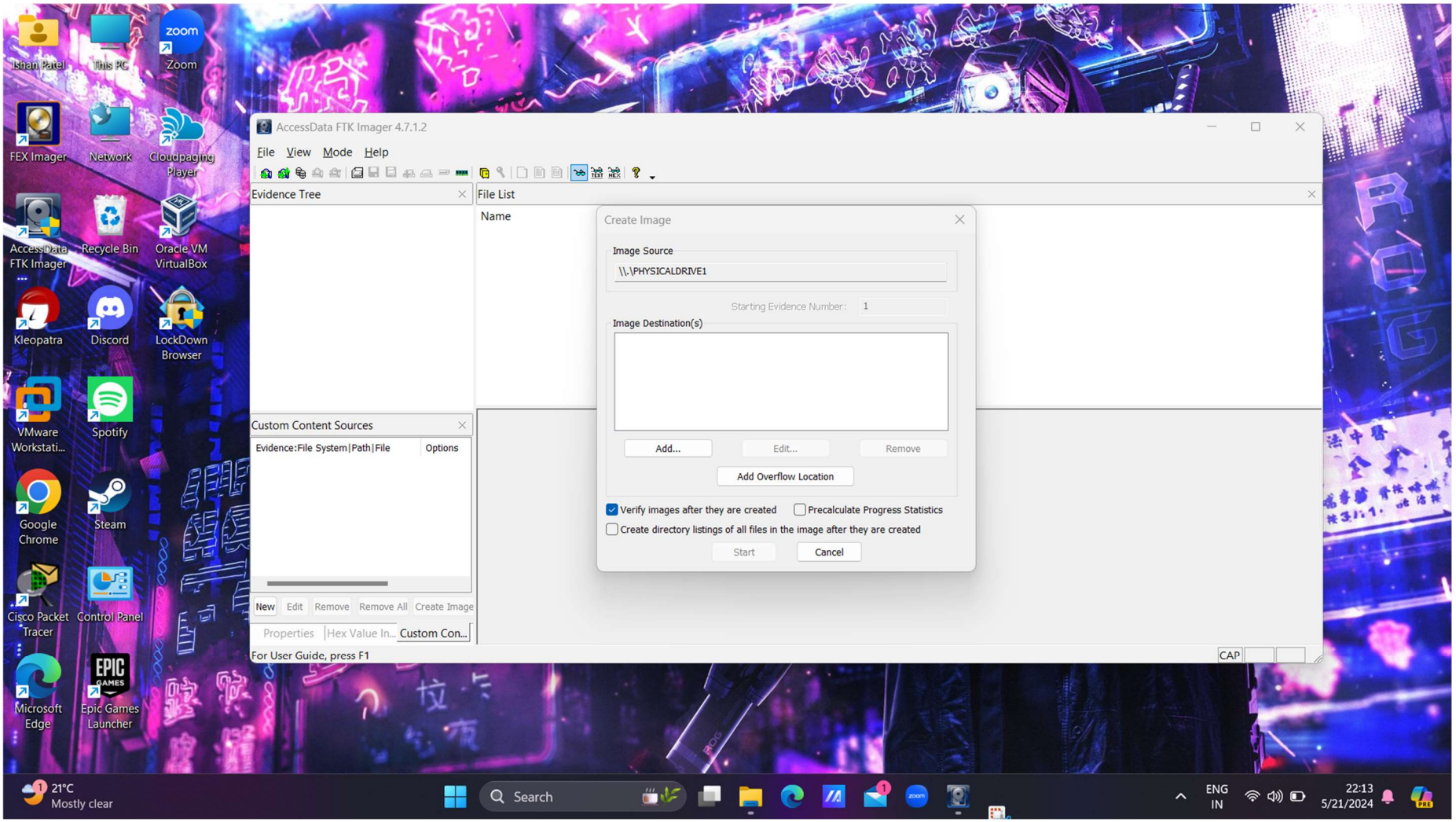


I am going to make an image of a flash – drive which I inserted.

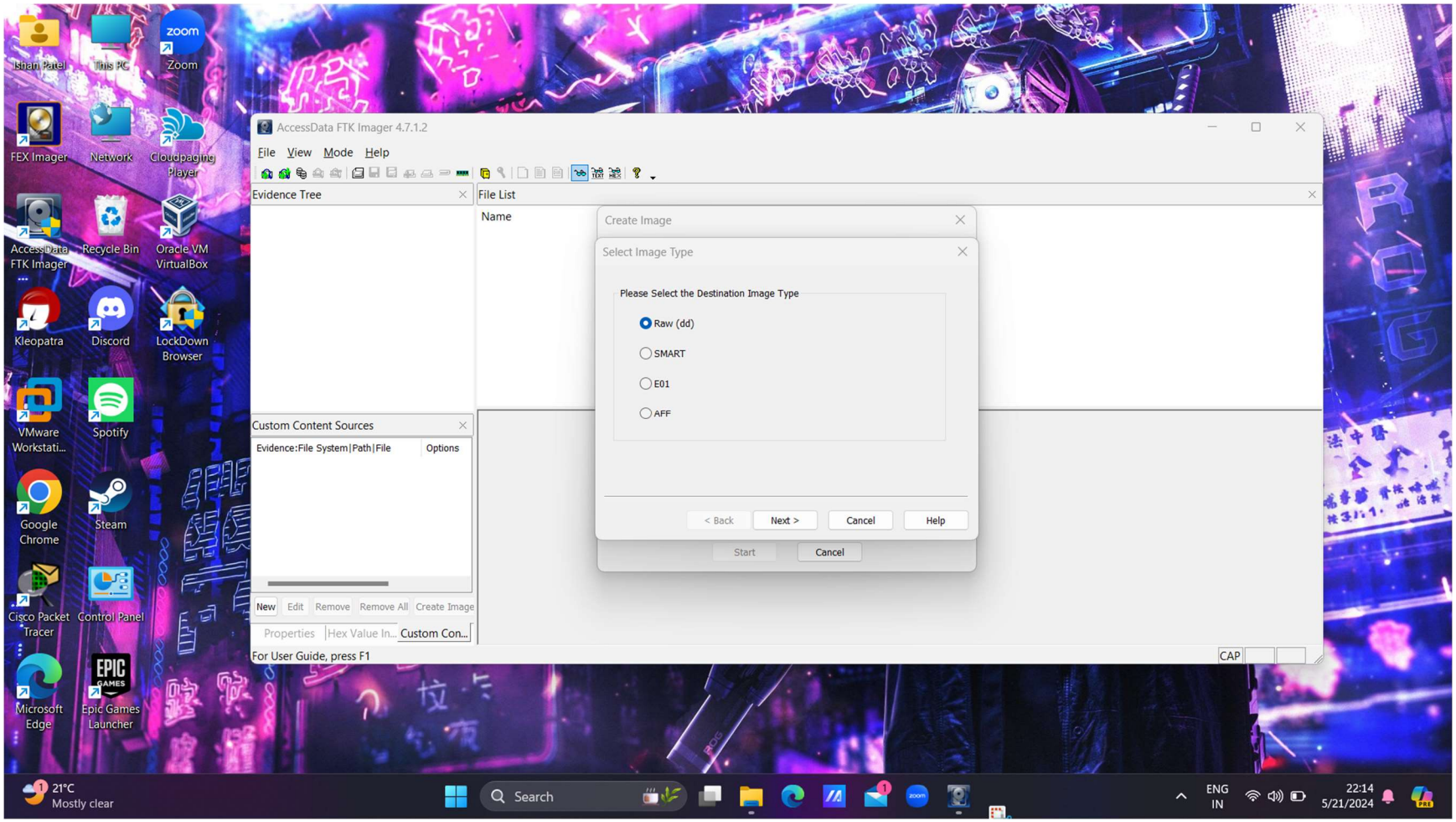


Here just what kind of drive you are selecting (Source). I selected Physical as I inserted a physical drive. In the next screenshot you can see that I have selected the pendrive.

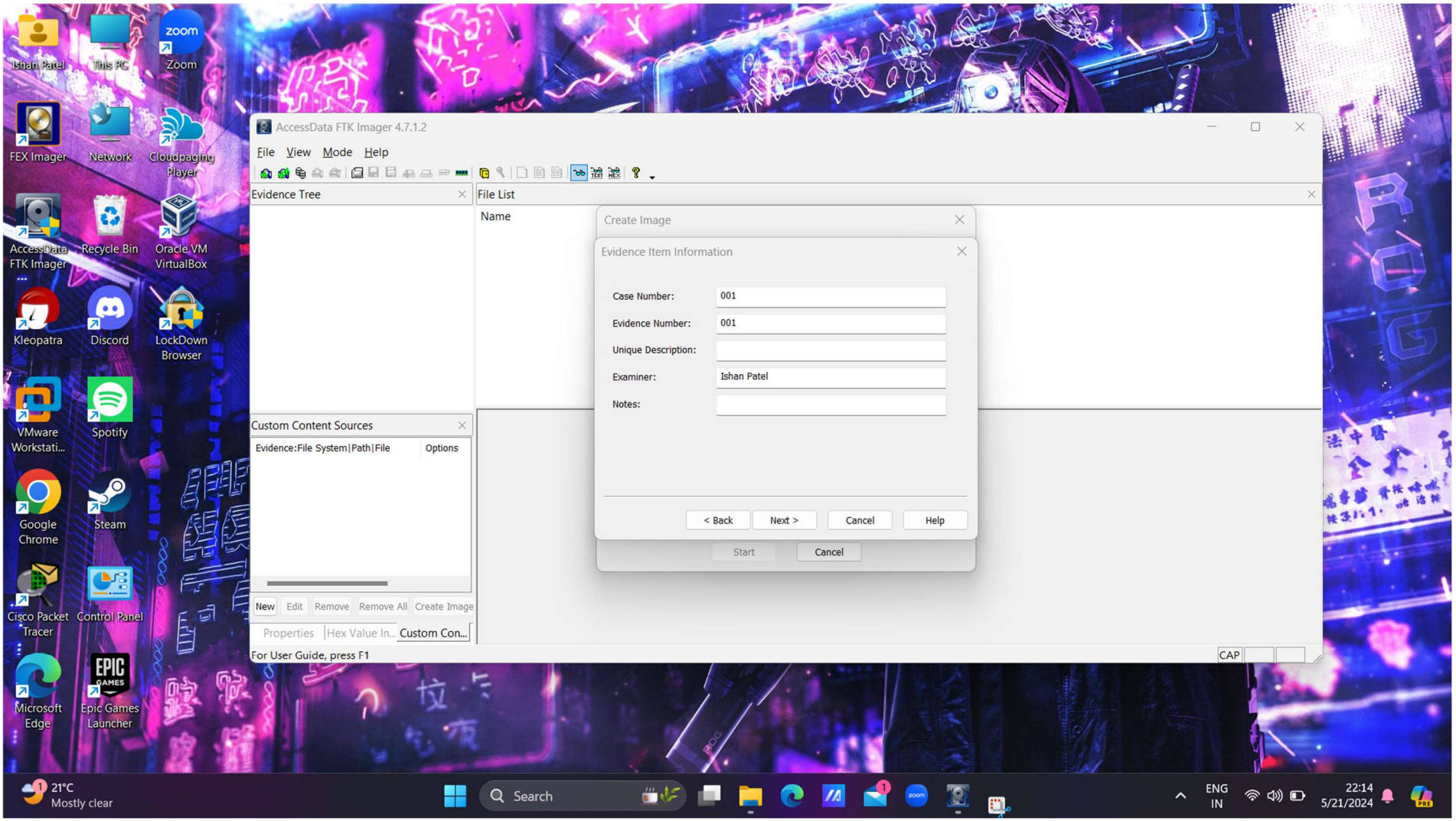

Ishan Patel
This PC
Zoom
FEX Imager
Network
Cloudpaging Player
AccessData FTK Imager
Recycle Bin
Oracle VM VirtualBox
Kleopatra
Discord
LockDown Browser
VMware Workstati...
Spotify
Google Chrome
Steam
Cisco Packet Tracer
Control Panel
Microsoft Edge
Epic Games Launcher
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - SanDisk Cruzer Blade USB Device [123GB US
< Back
Finish
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
For User Guide, press F1
CAP
21°C
Mostly clear
Search
ENG
IN
22:13
5/21/2024

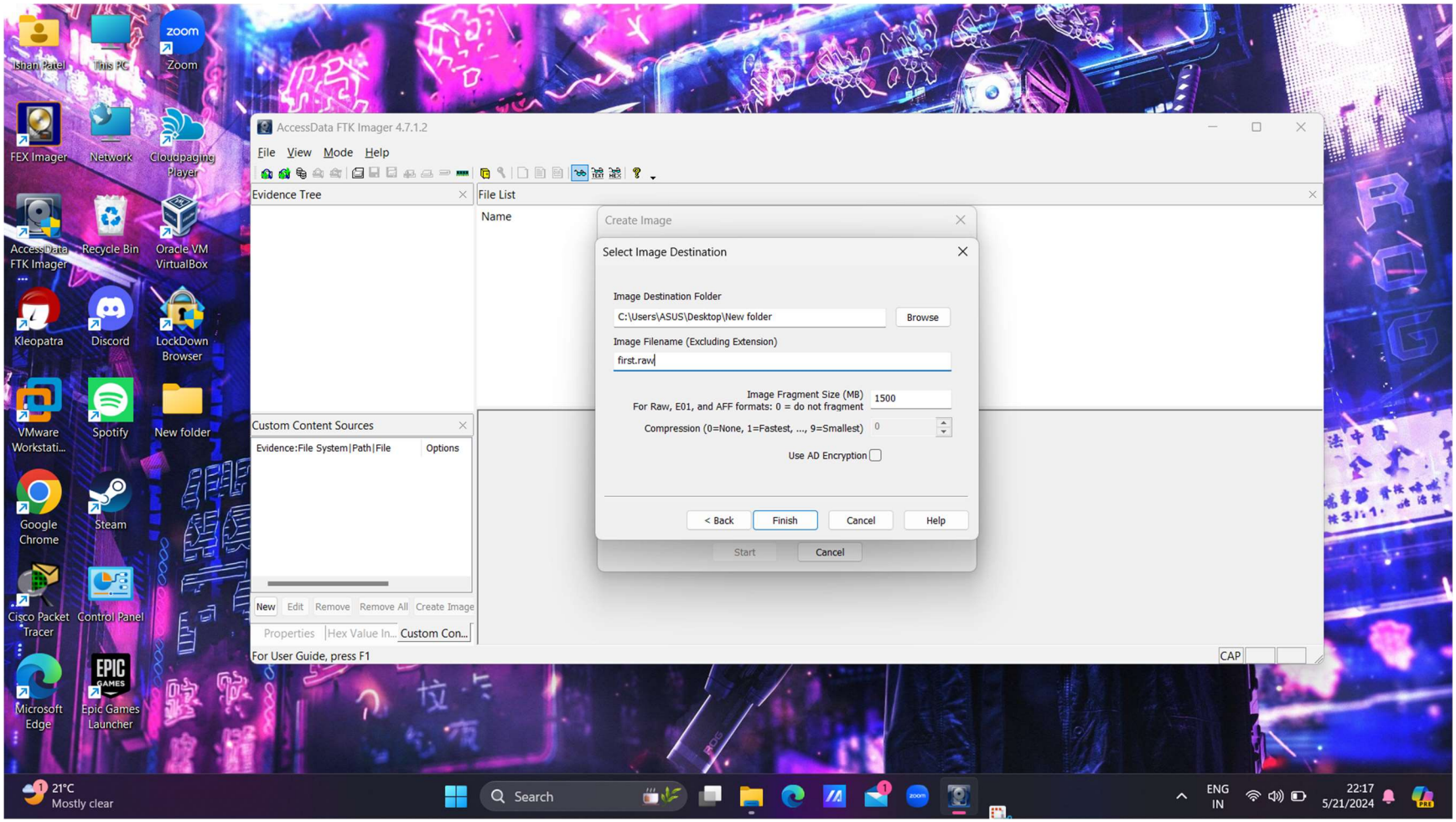


Now we need a destination where our image can be stored. Usually it is a empty pendrive / harddrive or ssd (in real world scenarios) but I don't have another one, So right now I will be saving it to my laptop.

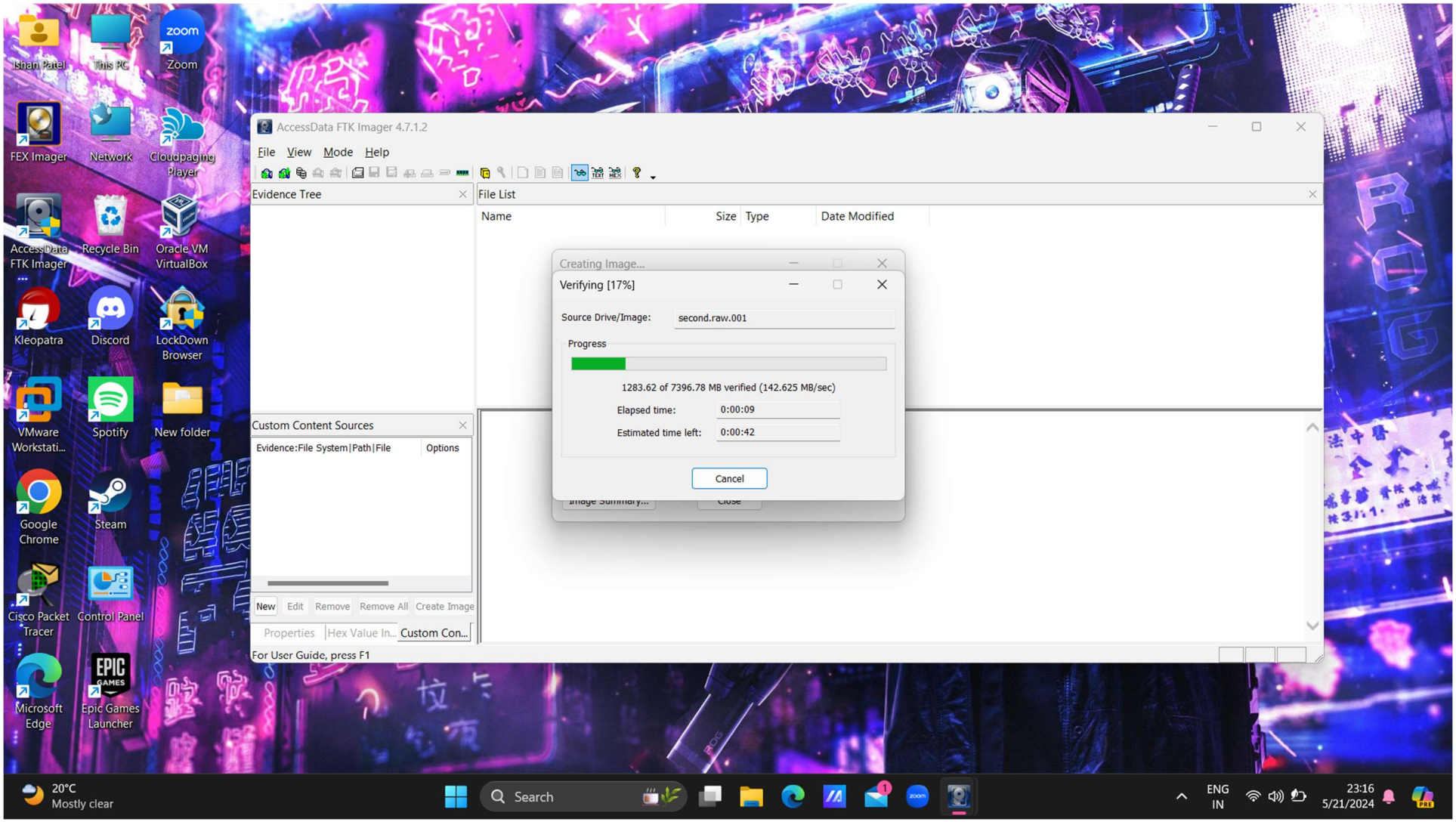


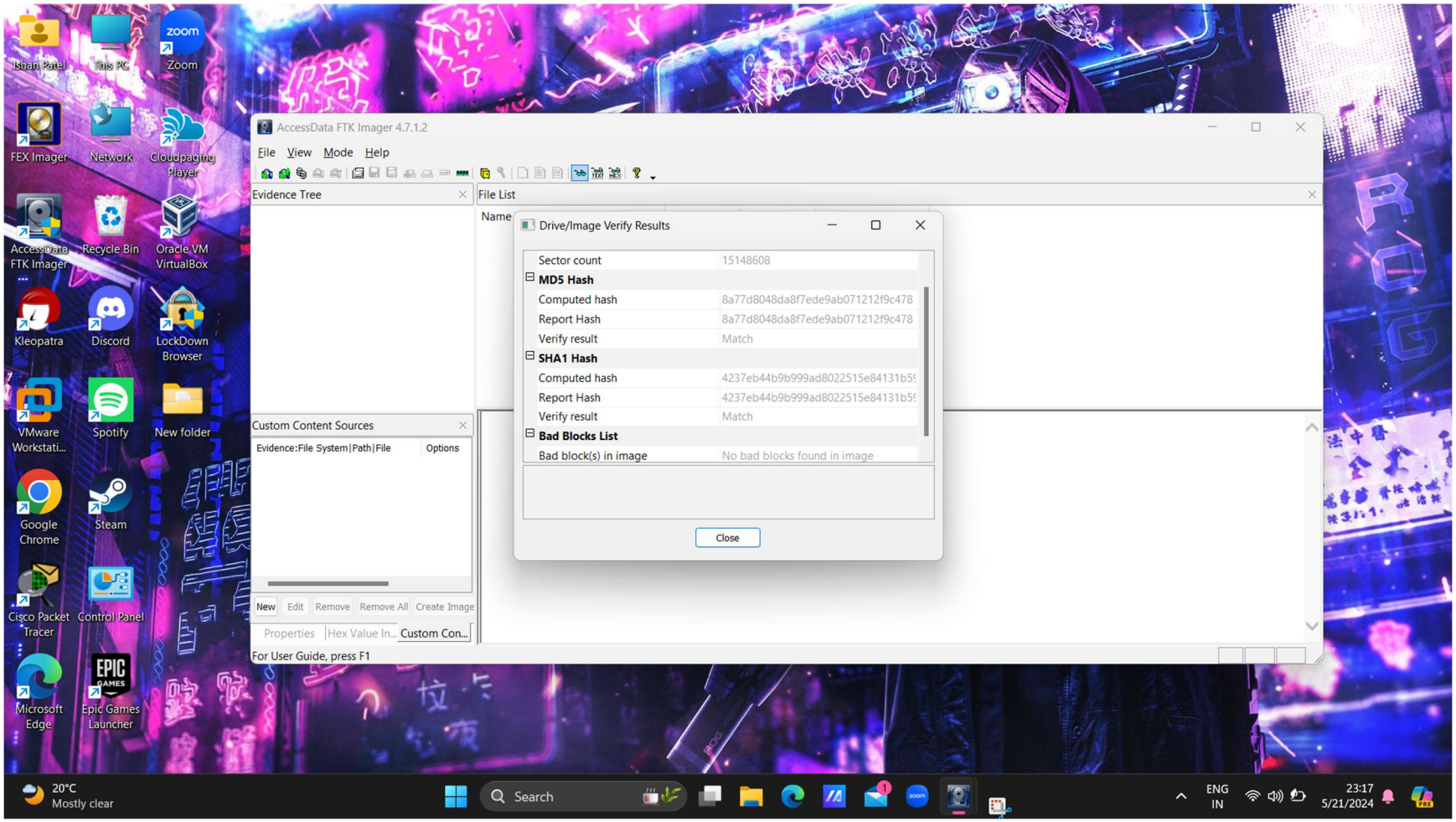
Select the image type – I selected raw image. Also in the next screenshot add the general description of the image like examiner, description, case number, etc.


Ishan Patel
This PC
Zoom
FEX Imager
Network
Cloudpaging Player
AccessData FTK Imager
Recycle Bin
Oracle VM VirtualBox
Kleopatra
Discord
LockDown Browser
VMware Workstati...
Spotify
Google Chrome
Steam
Cisco Packet Tracer
Control Panel
Microsoft Edge
Epic Games Launcher
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Create Image
Evidence Item Information
Case Number: 001
Evidence Number: 001
Unique Description:
Examiner: Ishan Patel
Notes:
< Back
Next >
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
For User Guide, press F1
CAP
21°C
Mostly clear
Search
ENG
IN
22:14
5/21/2024



Here I selected the destination of the image were I am currently saving and also give the name to the image. Then, I started the process and as my pendrive was bit old its processing speed was very low. So, after 2 hours I canceled it and took my friend's pendrive which was of 8 GB. You can see this in next screenshot.


Ishan Patel
This PC
Zoom
FEX Imager
Network
Cloudpaging Player
AccessData FTK Imager
Recycle Bin
Oracle VM VirtualBox
Kleopatra
Discord
LockDown Browser
VMware Workstati...
Spotify
New folder
Google Chrome
Steam
Cisco Packet Tracer
Control Panel
Microsoft Edge
Epic Games Launcher
AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Creating Image...
Verifying [17%]
Source Drive/Image:
second.raw.001
Progress
1283.62 of 7396.78 MB verified (142.625 MB/sec)
Elapsed time:
0:00:09
Estimated time left:
0:00:42
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value In...
Custom Con...
For User Guide, press F1
20°C
Mostly clear
Search
ENG
IN
23:16
5/21/2024



Here you can see that image verify results are a match both in MD5 hash as well as SHA1 hash. So, it means that it's the same image and its not be altered – its integrity is intact.

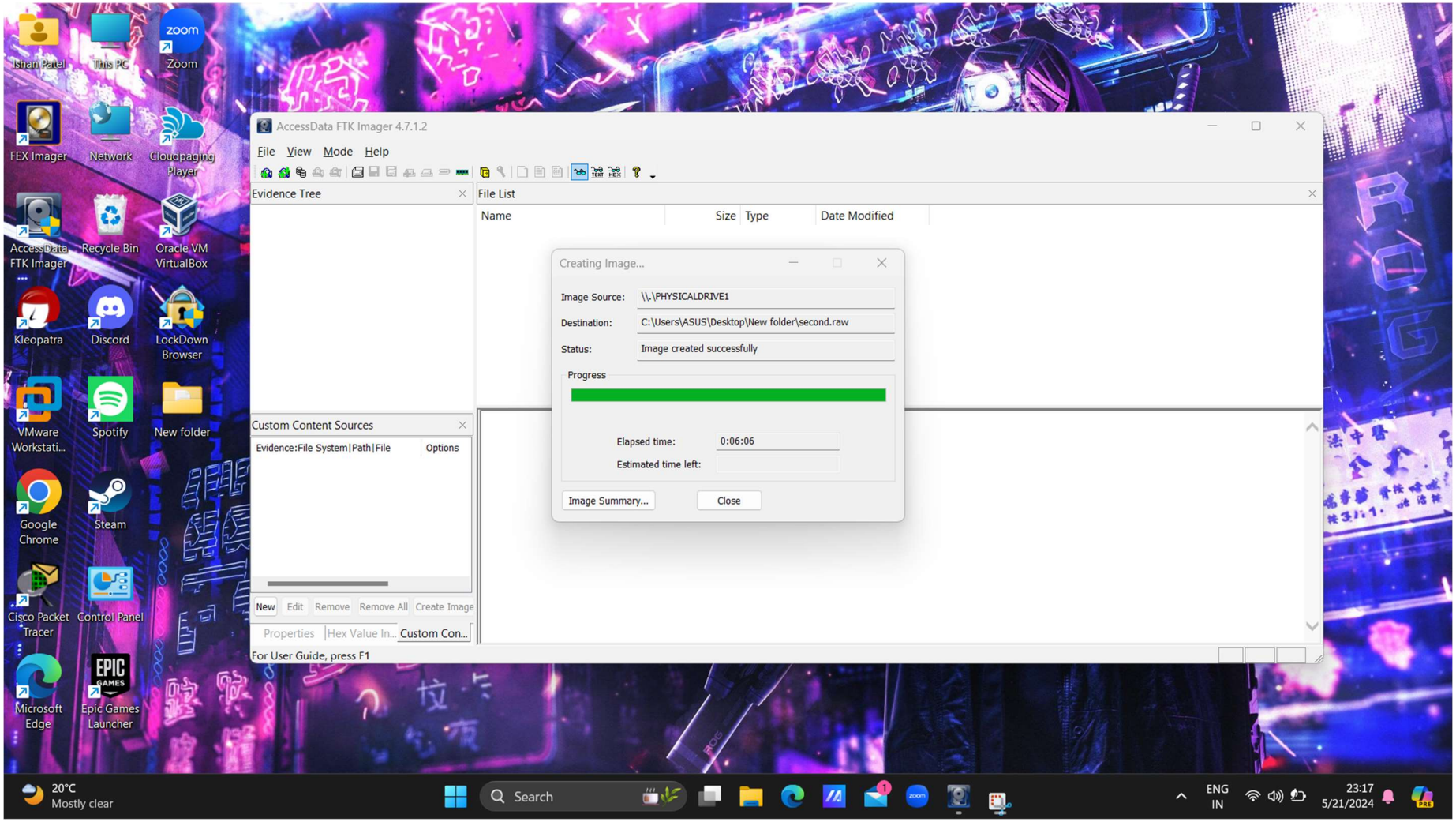
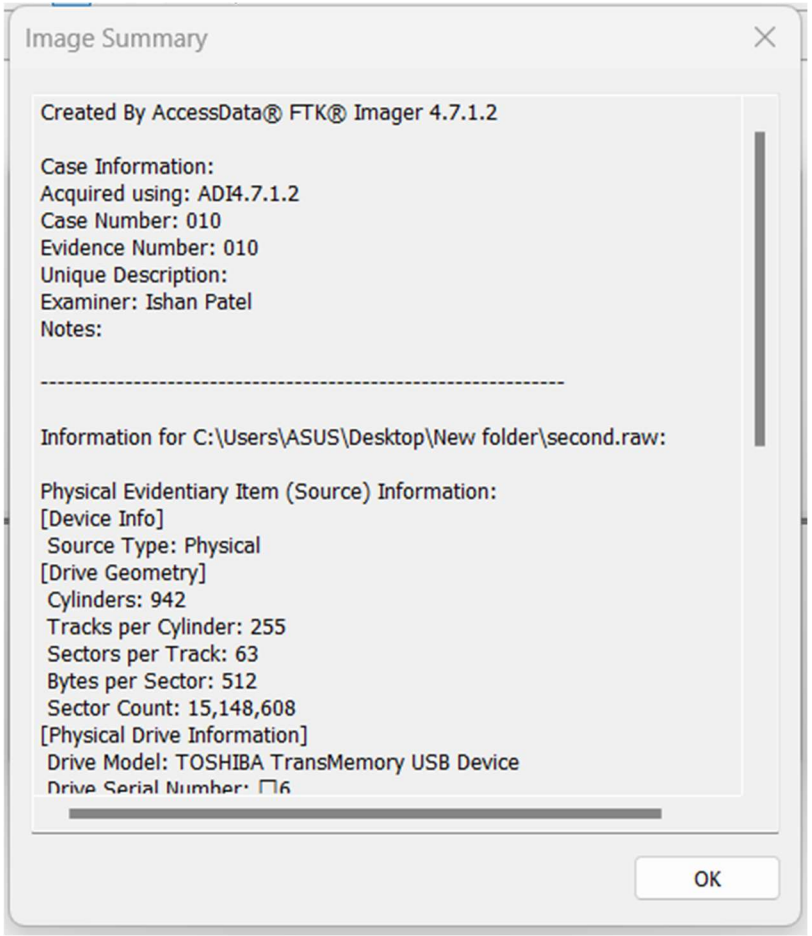
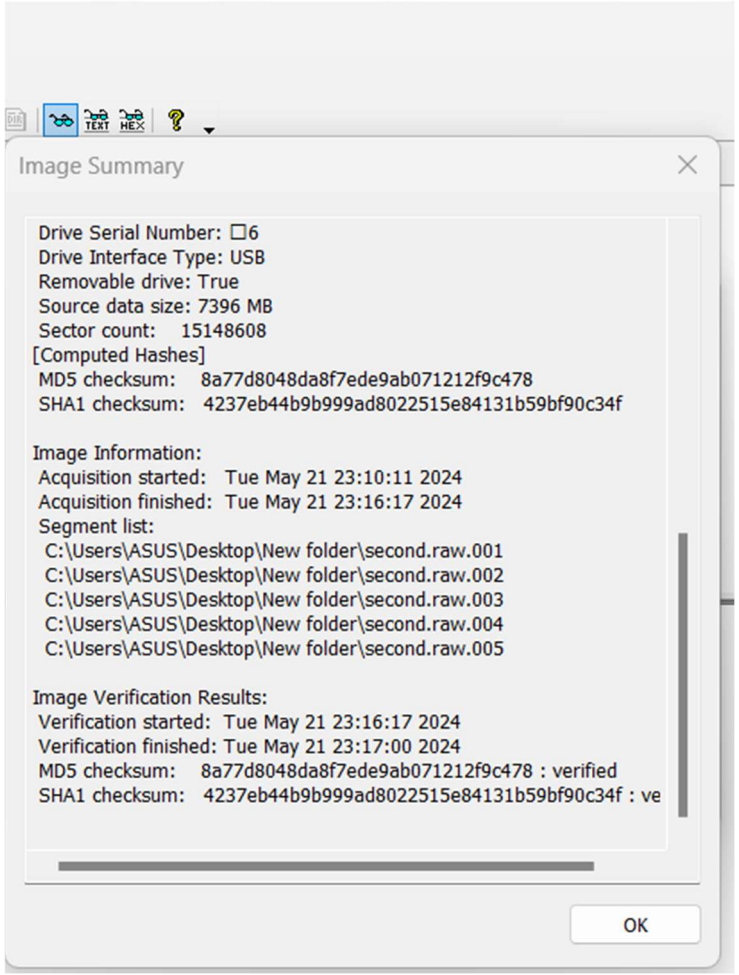


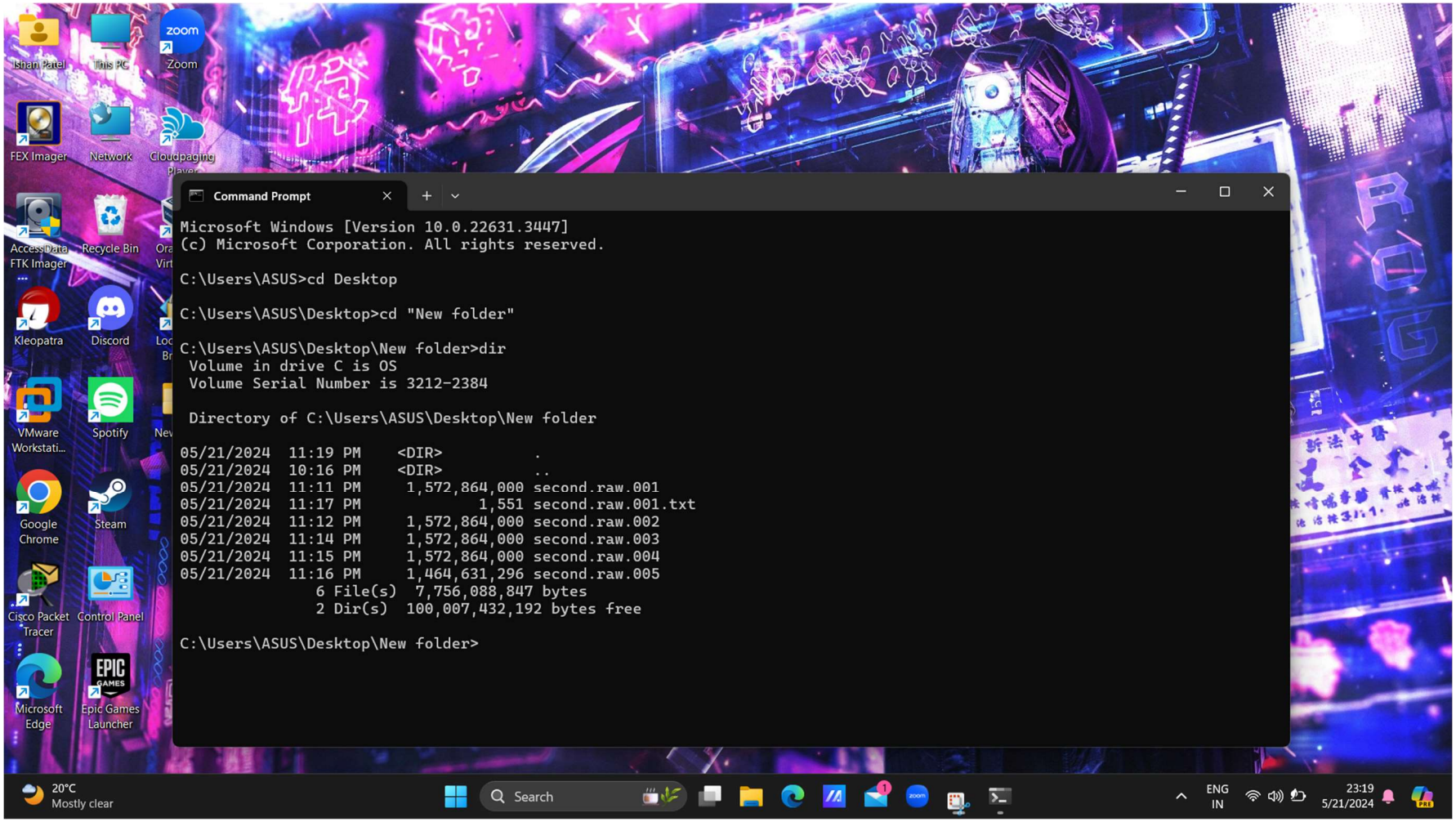
Image created sucessufully.

Here you can see the image summary which gives you much more details.



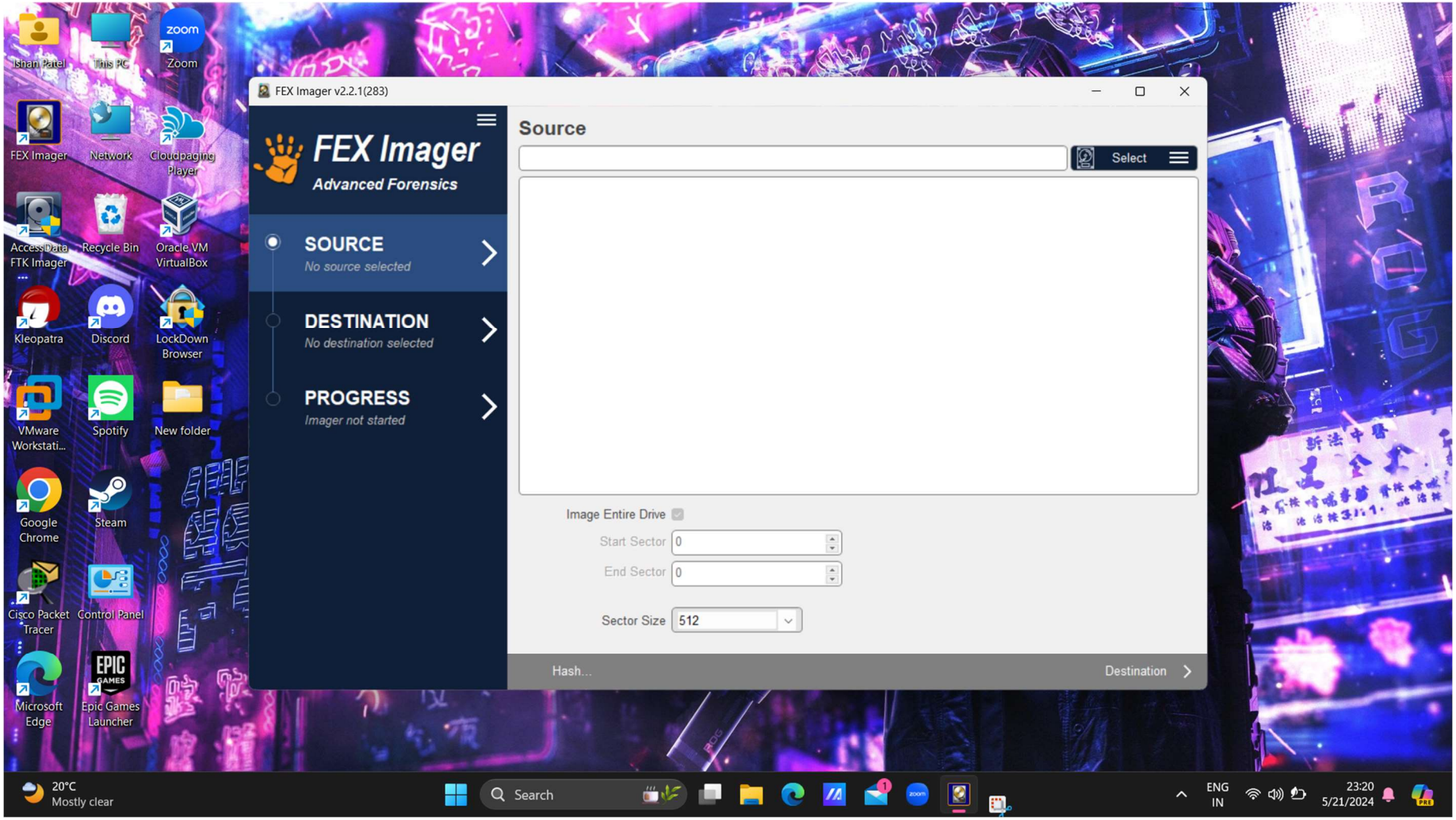


Proof of the image:



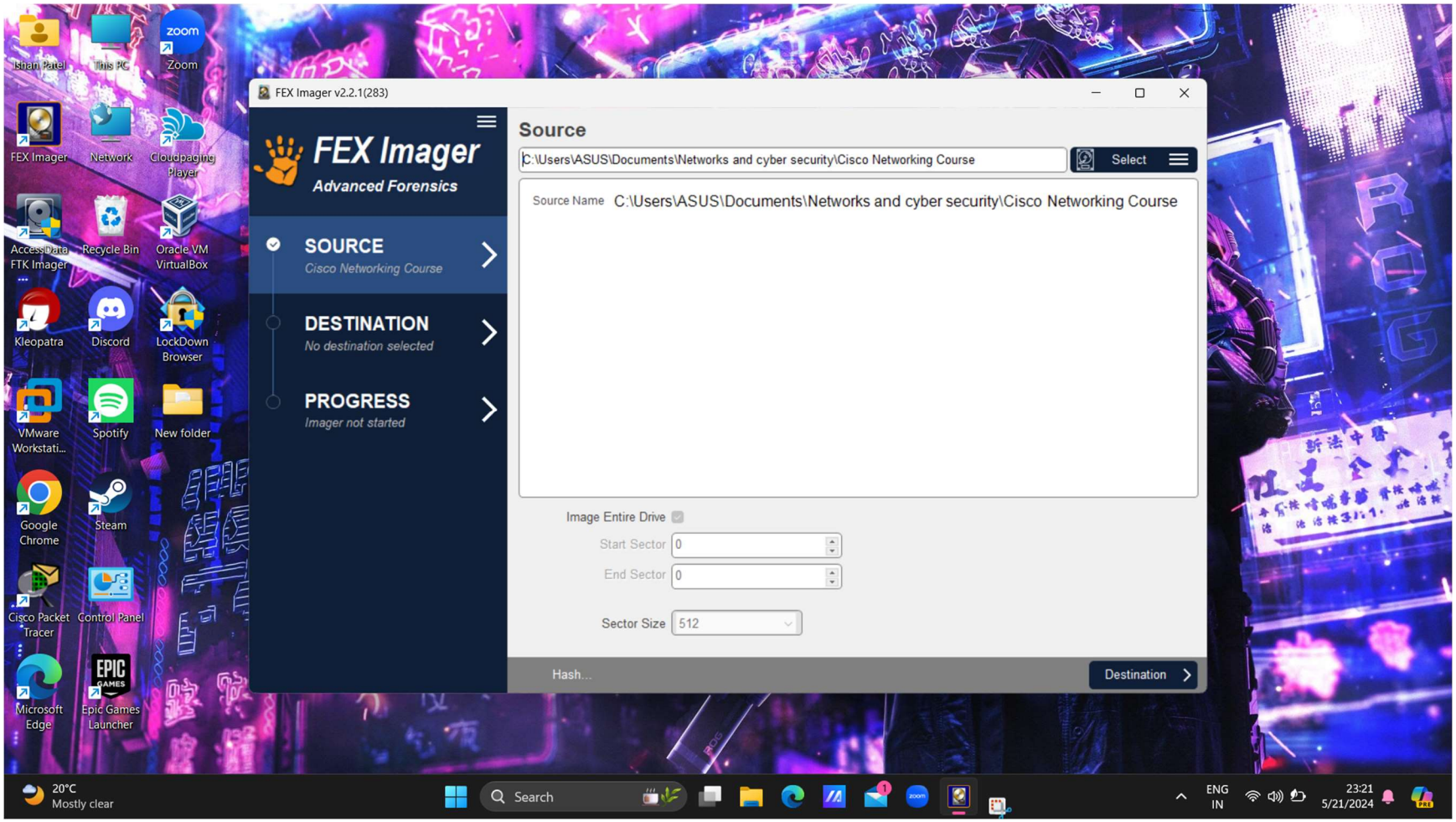
Tool 2 – Forensics Imager

I install the tool by the link given in the lab description.



In this tool I was not able to select any specific drive or pen drive. So, I selected a folder.

Here is the folder that I selected.



In the destination – Select the folder were you want to save it and also add some other details about the image.

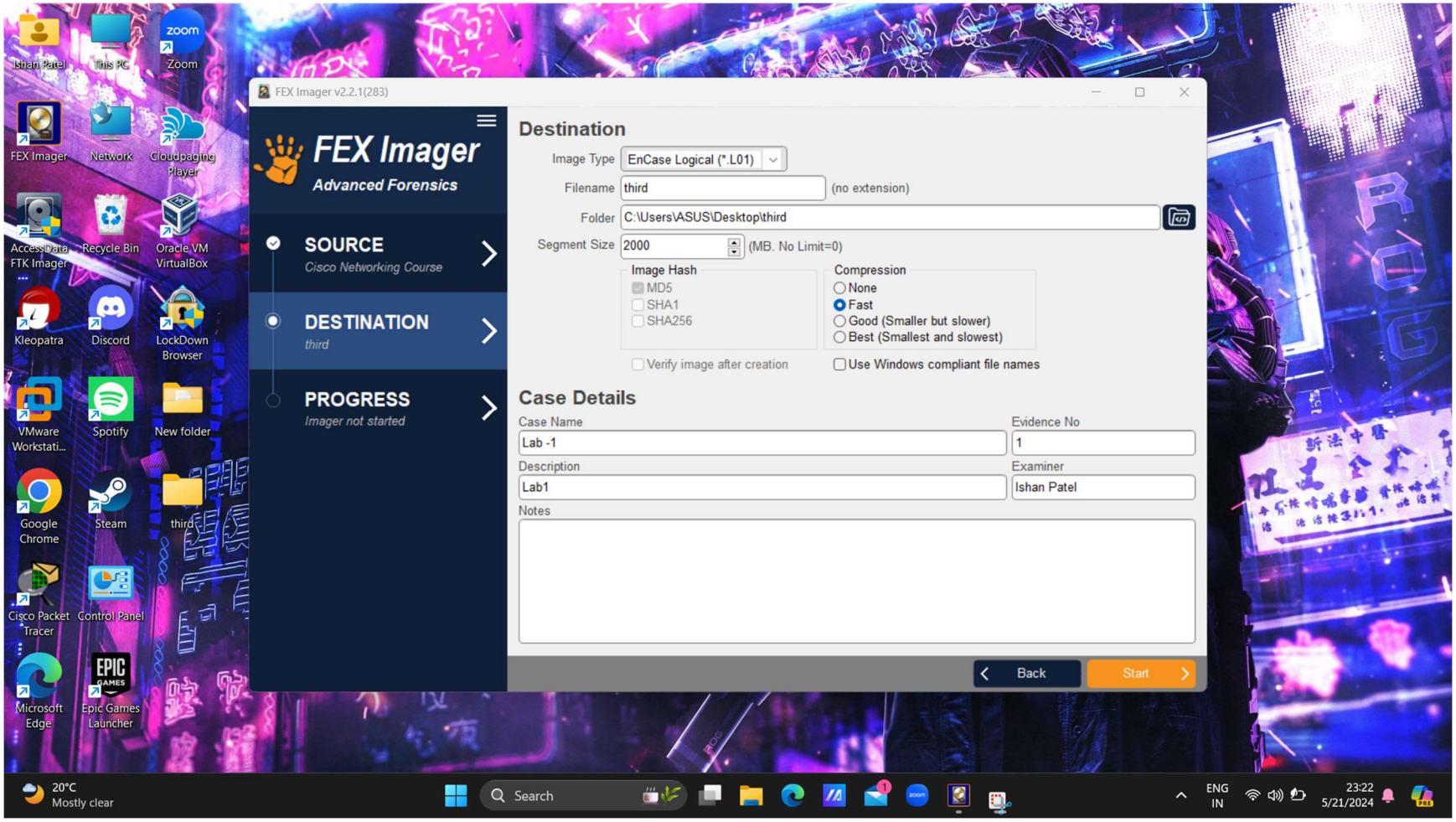
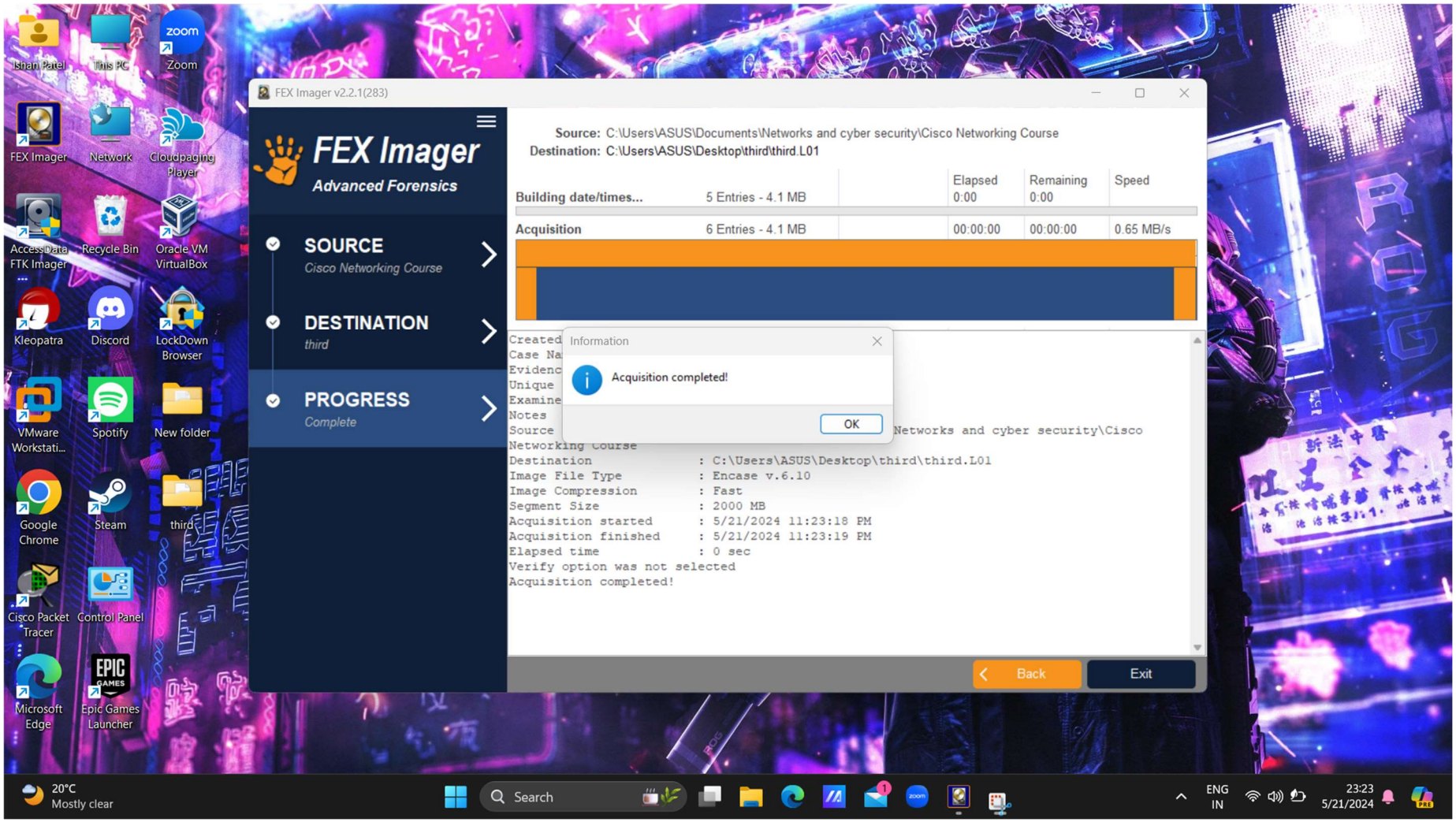
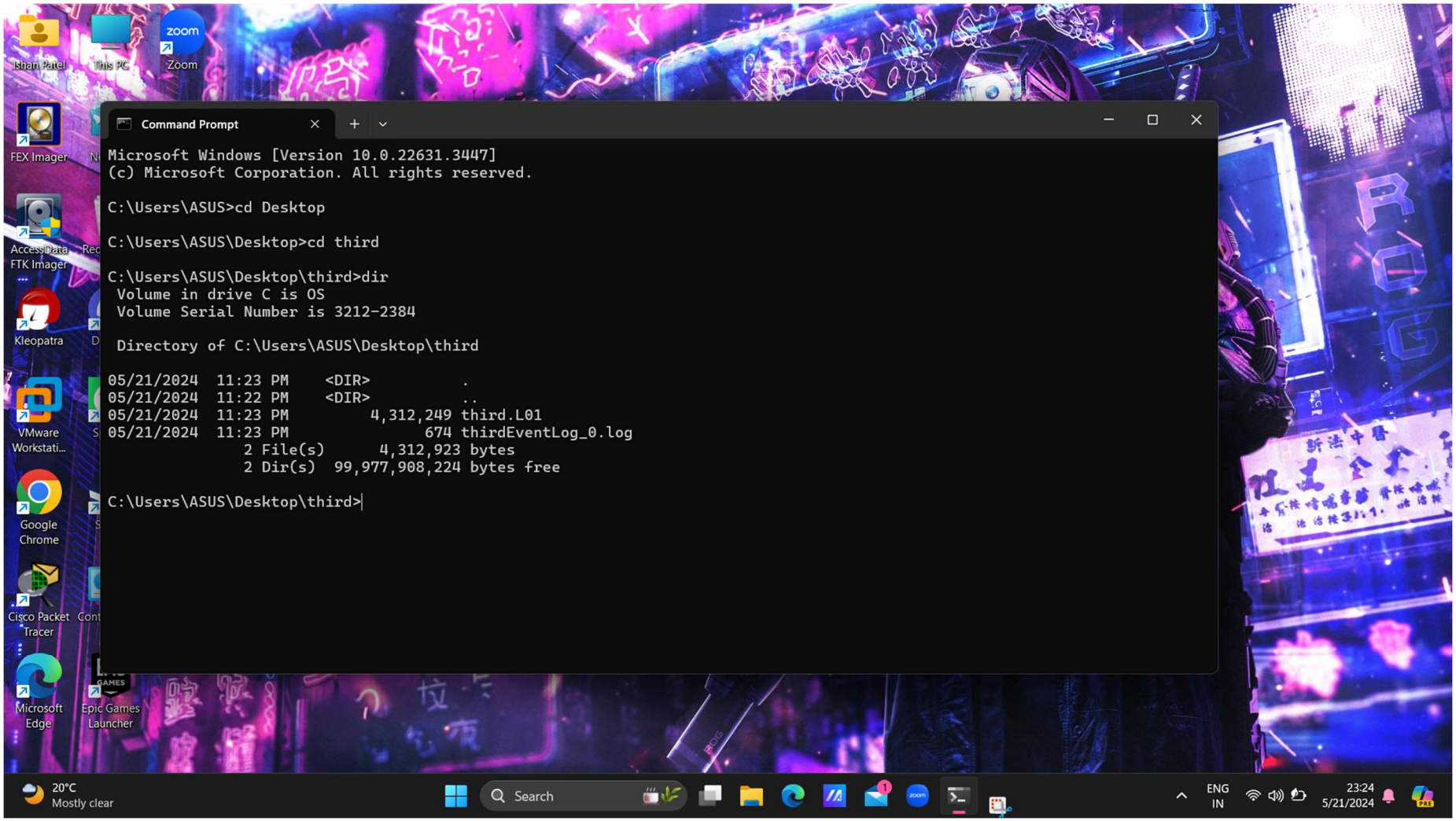


Image created successfully.



Proof of the Image :



Questions

1) Which Tool is Good and Easy to Use?

FTK Imager was found to be better and easier to use. Its interface is more intuitive, and it provides more options and flexibility during the imaging process. It also offers built-in verification features that make it easier to ensure the integrity of the created image.

2) How to Verify that Your Image is Correct?

To verify that your image is correct:

a) Checksum Verification:

Both tools generate a checksum (MD5 or SHA-1 hash) during the imaging process.

After creating the image, compare the checksum of the original disk with the checksum of the image. They should match exactly.

b) Image Loading:

Load the created image into forensic analysis software (like FTK Imager itself).

Verify that the image loads correctly and that all files and directories are accessible.

Learning Experience

Using both FTK Imager and Forensic Imager was a great learning experience. It taught me how to create disk images, which are exact copies of a computer's hard drive, for forensic analysis. I learned how to navigate the user interfaces of both tools, select the correct drive to image, choose the appropriate file format, and start the imaging process. Additionally, I understood the importance of verifying the created image using checksums to ensure its accuracy. Overall, it was an insightful exercise that showed me the practical steps involved in digital forensics and the importance of precise and reliable tools in this field.