Name: Ghulam Abbas

Roll No: 030

DEPT: DFRC

Assignment1 Part-B Submitted to: -

Miss Fatima

Q1: What are the necessary steps that must be followed before creating forensic images of source devices?

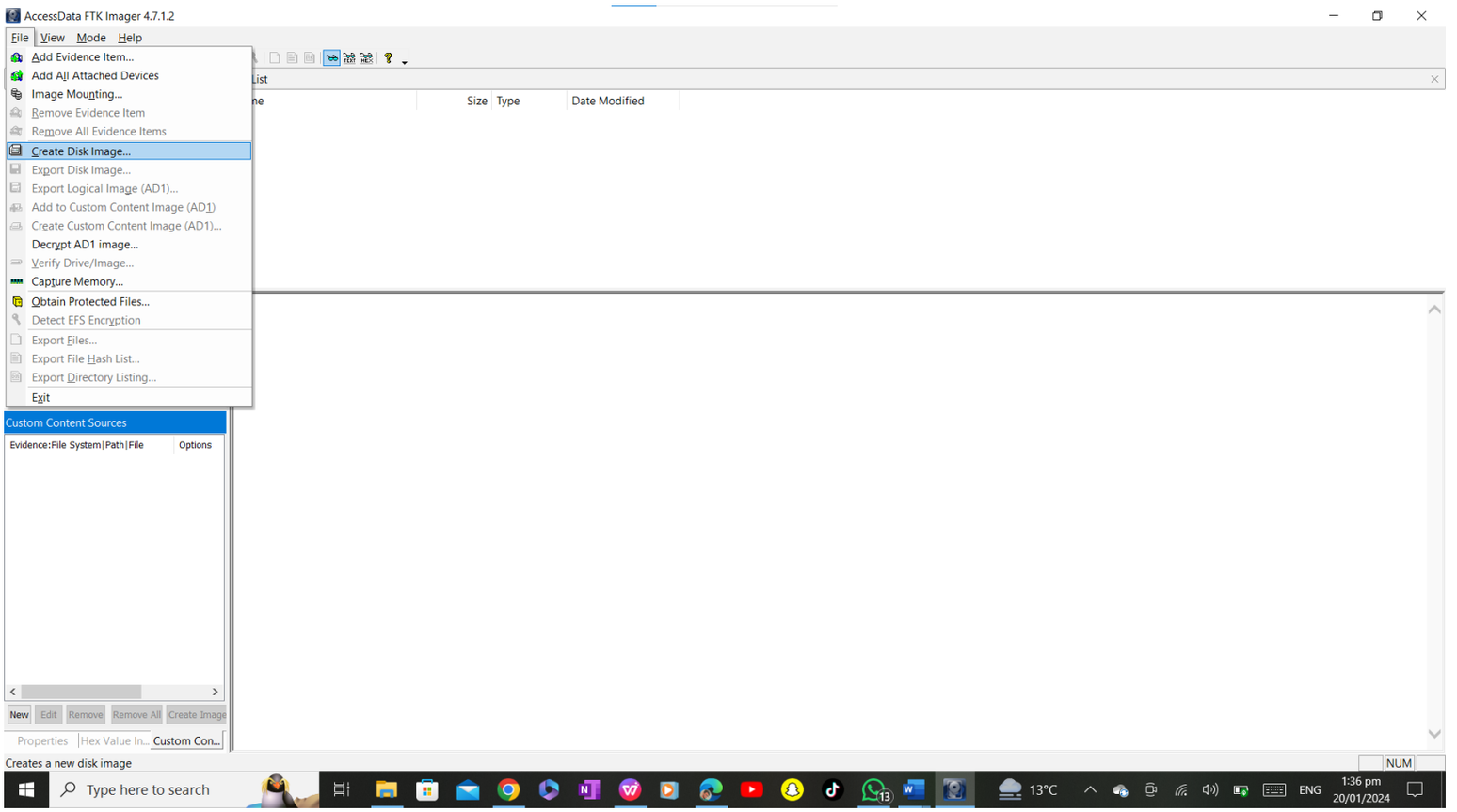
Ans: Here are the steps that should be taken before creating forensic images of source devices:

1. **Documentation and Planning:**
- Document details about the case, including the nature of the investigation, legal requirements, and specific devices involved.
- Plan the imaging process, considering the type of devices, storage media, and any potential challenges.
2. **Chain of Custody:**
- Establish and maintain a chain of custody to document the handling, storage, and transfer of the evidence. This is crucial for maintaining the integrity of the evidence in court.
3. **Verification of Tools:**
- Verify the integrity of the forensic tools by comparing hash values against known and trusted values. This ensures that the tools have not been compromised and will not alter the data during imaging.
4. **Preparation of Target Media:**
- Prepare the target media (where the forensic image will be stored) ensuring it has enough capacity and is free from any existing data that may compromise the forensic image.
5. **Imaging Process:**

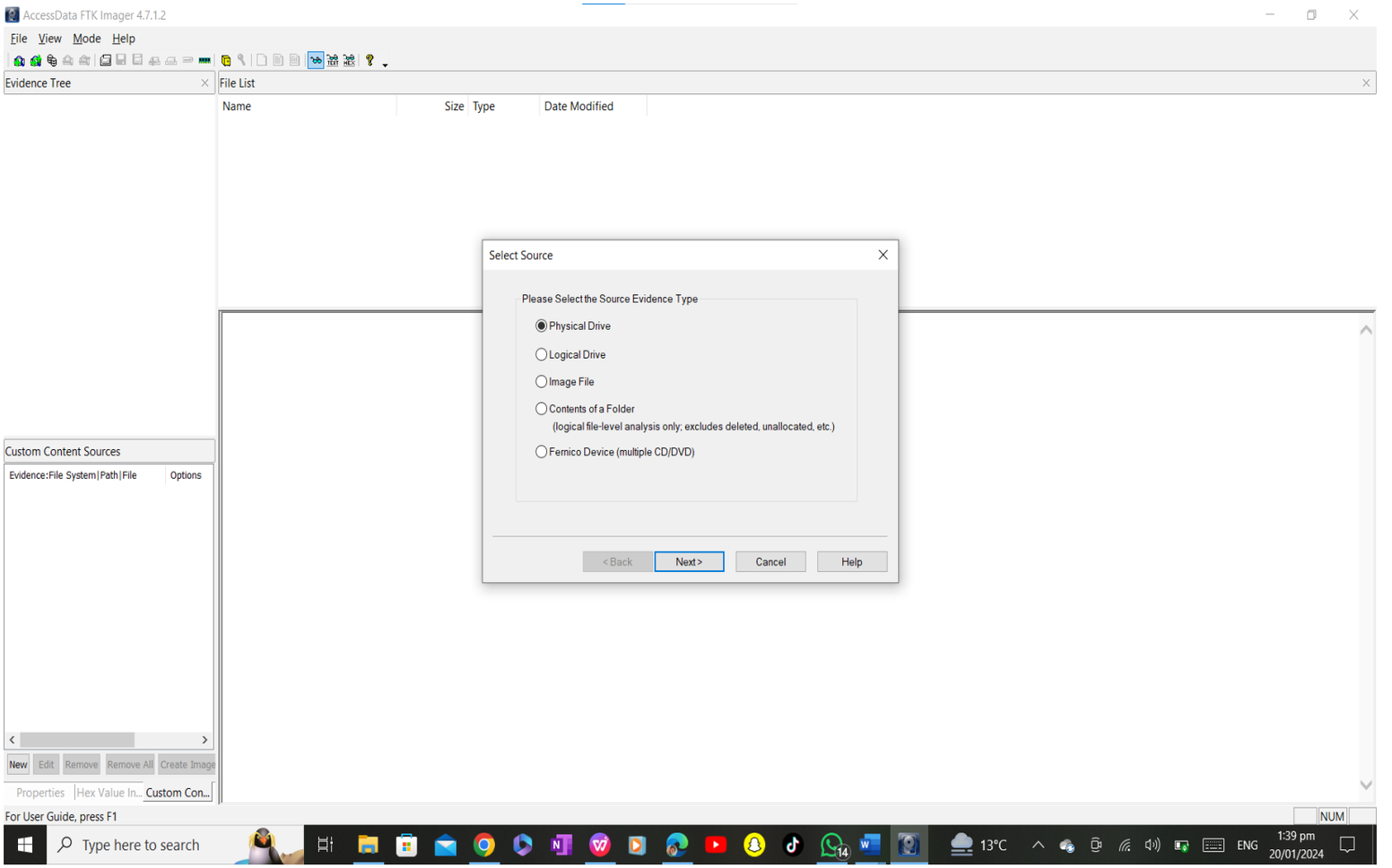
- Use a forensically sound imaging process to create a bit-for-bit copy of the source device. This ensures that all data, including deleted and hidden files, is preserved. Record relevant metadata during the imaging process, such as date, time, and details of the imaging tool used.

  Q2: Create forensic image of any source device e.g. disk/USB/SD cards etc. with title of your name using FTK or any other validated forensic tool (Situation-i).

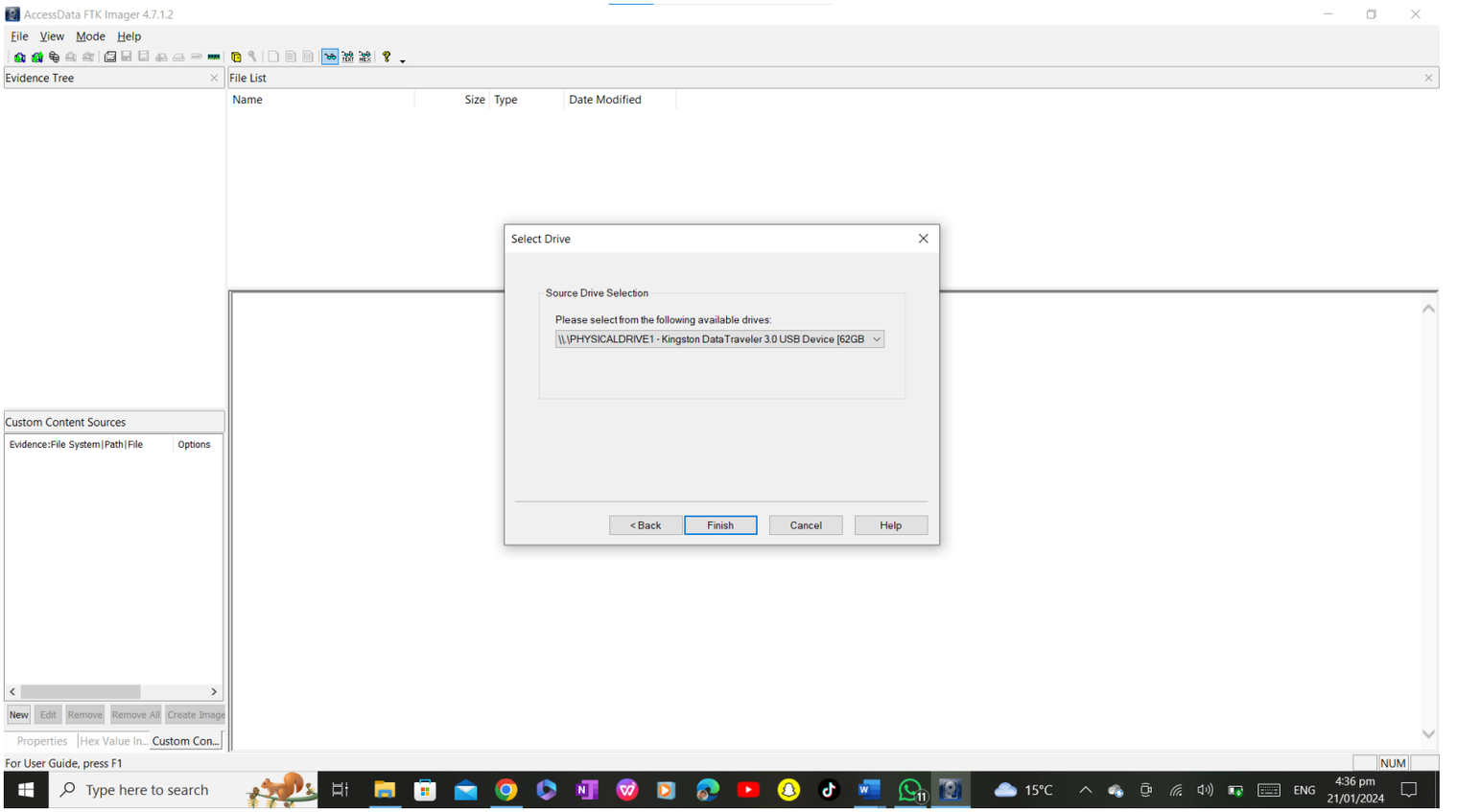
  First Open the FTK application click on file option and select create image disk.



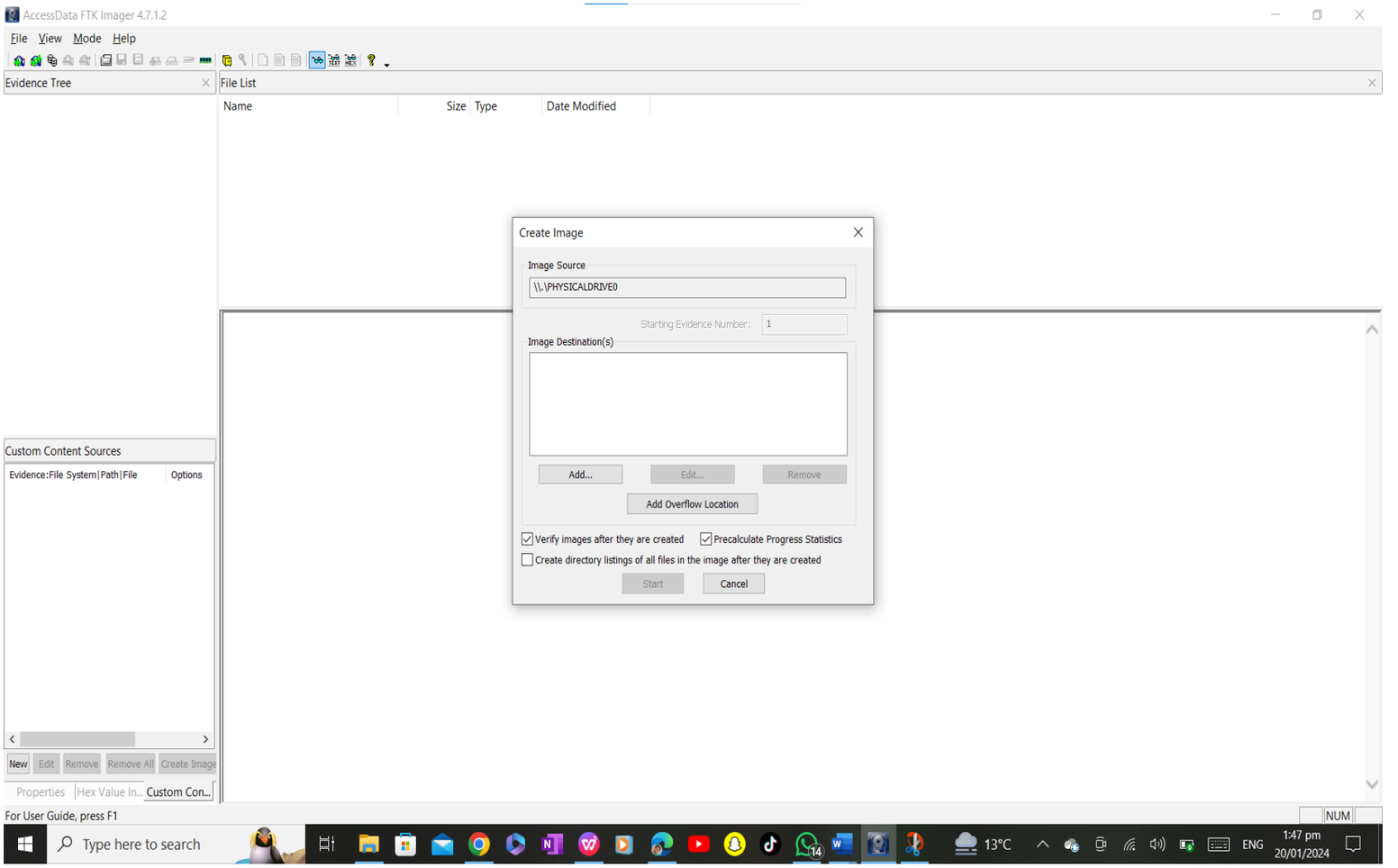
Here we can choose various types of source evidence. But in my case, I will choose physical drive because we will use USB or SD card.



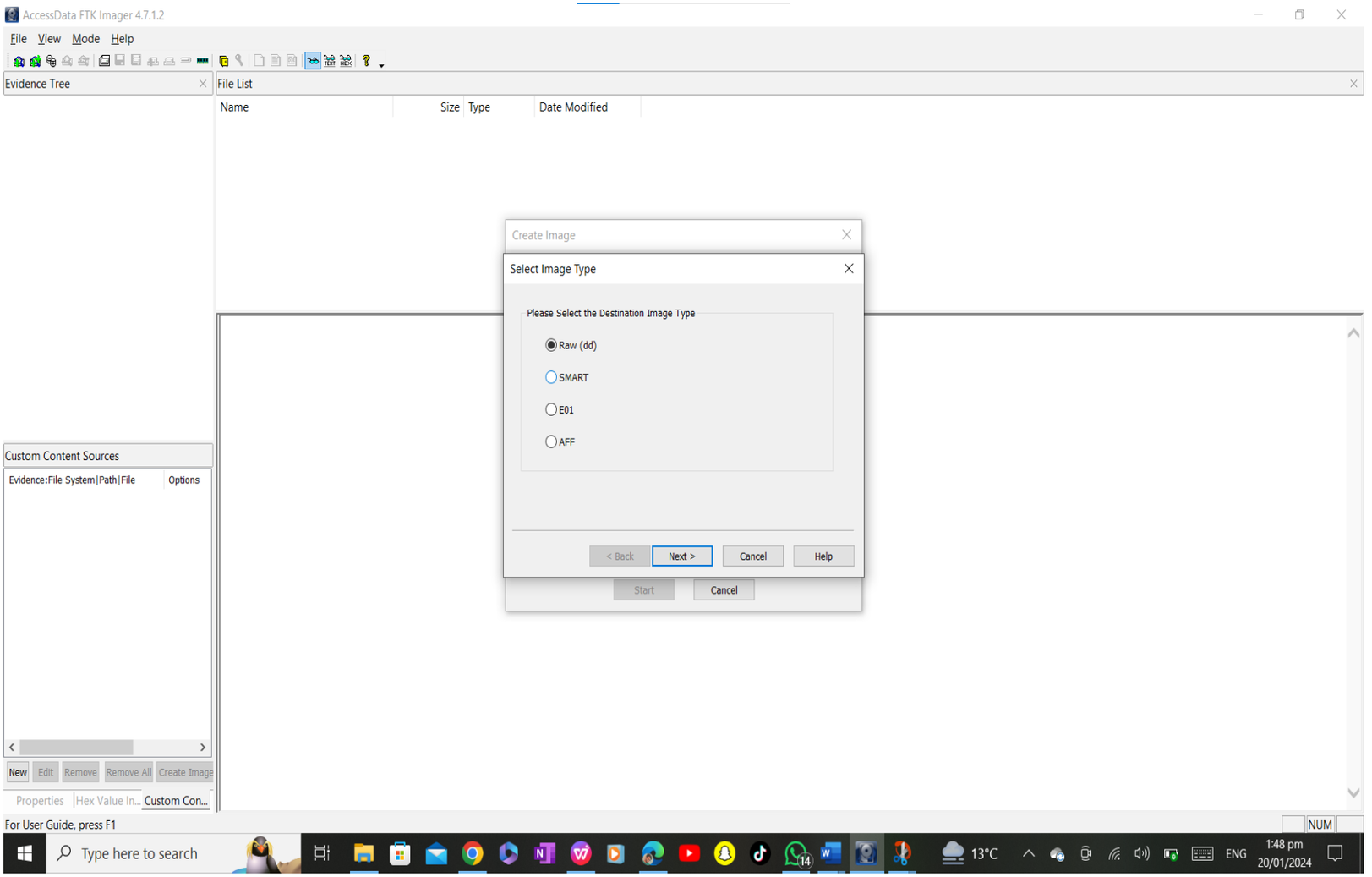
Selection the physical device it may be a USB or portable hard drive



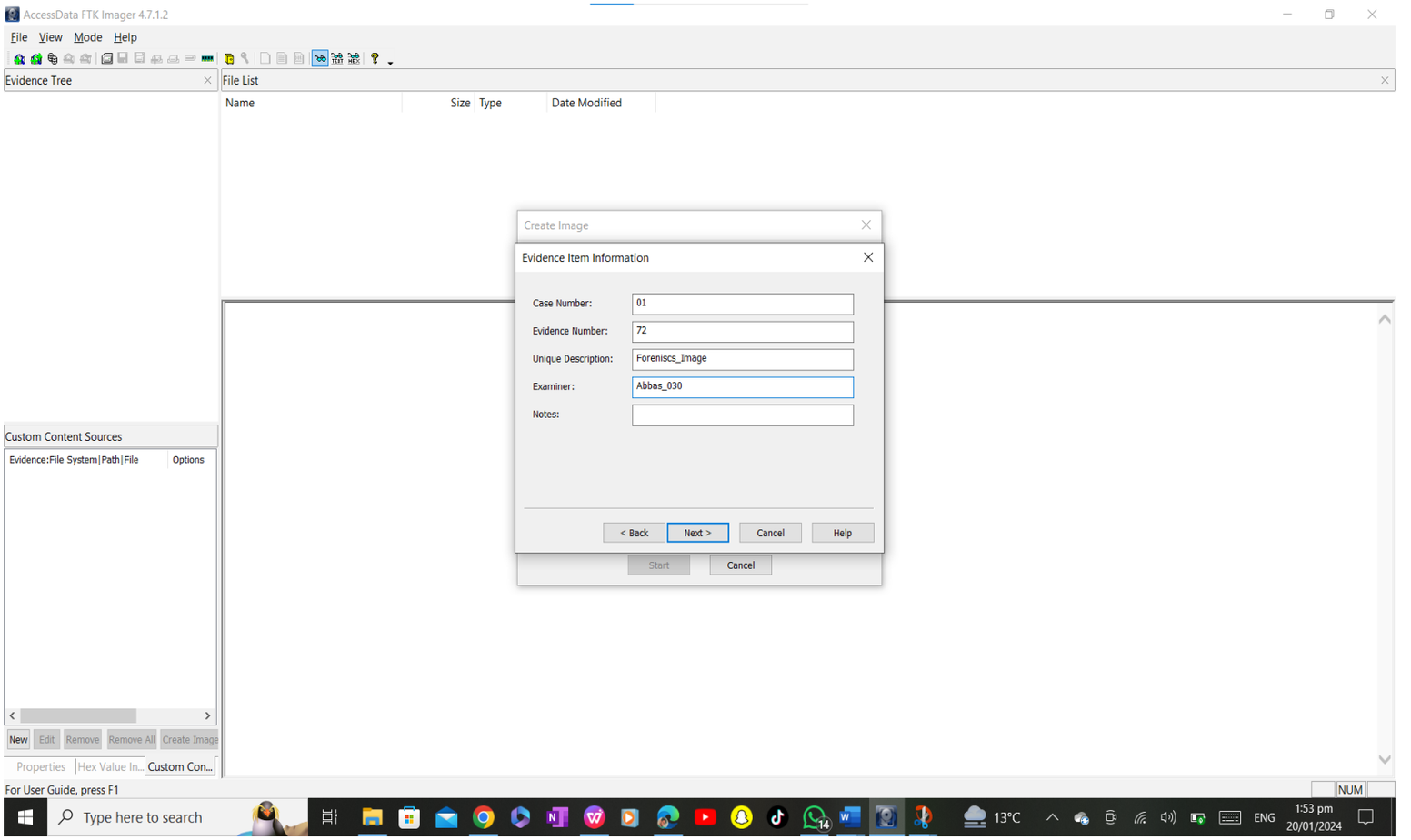
Here starts the image create processes



Here, we can select the other types of forensics image like Raw (dd) or Advance Forensic Format (AFF) etc. But I am selecting Raw(dd) because it is fast and mostly all the tools support it.

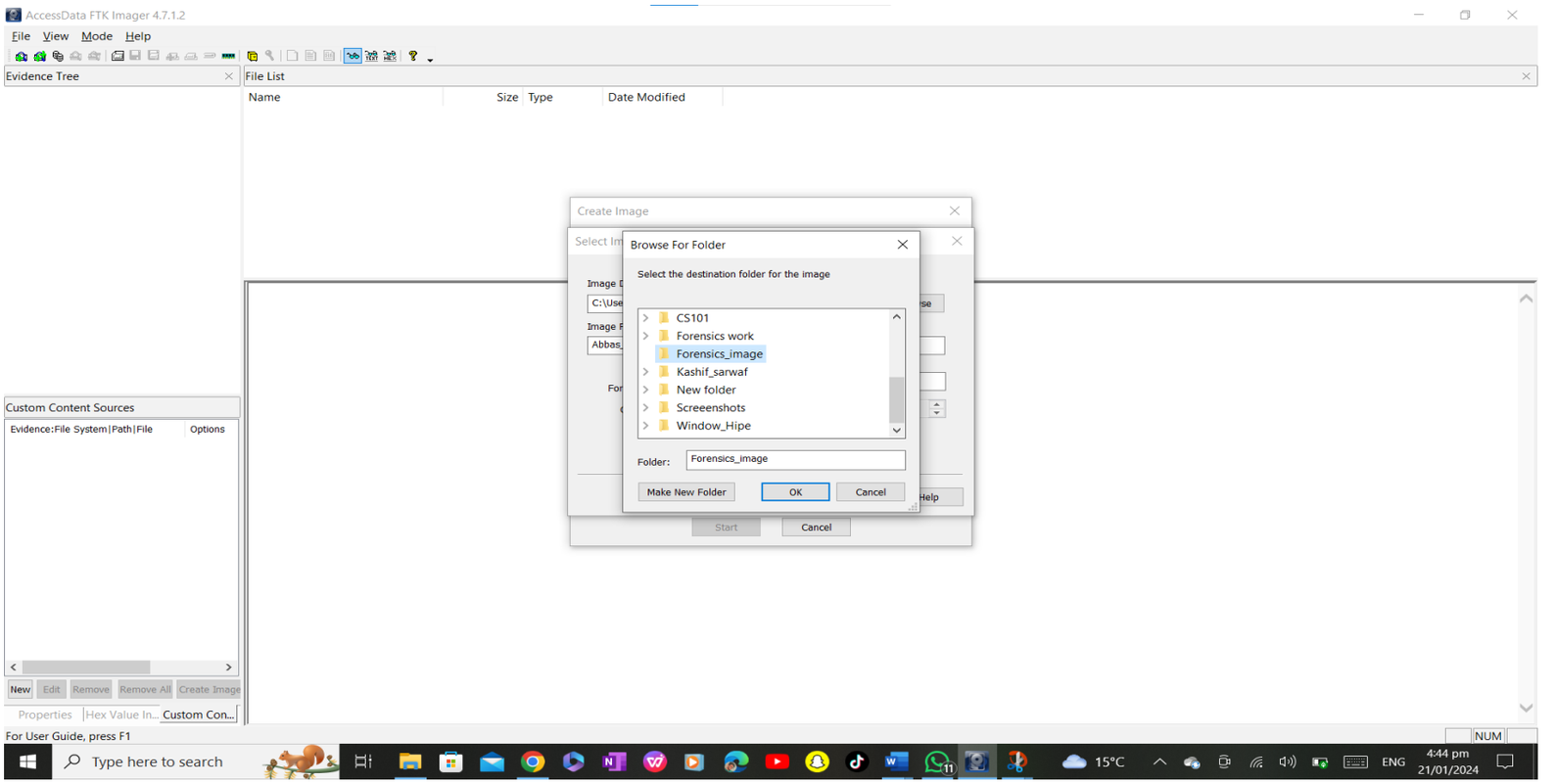


Here we are adding evidence information for searching case easily for him.

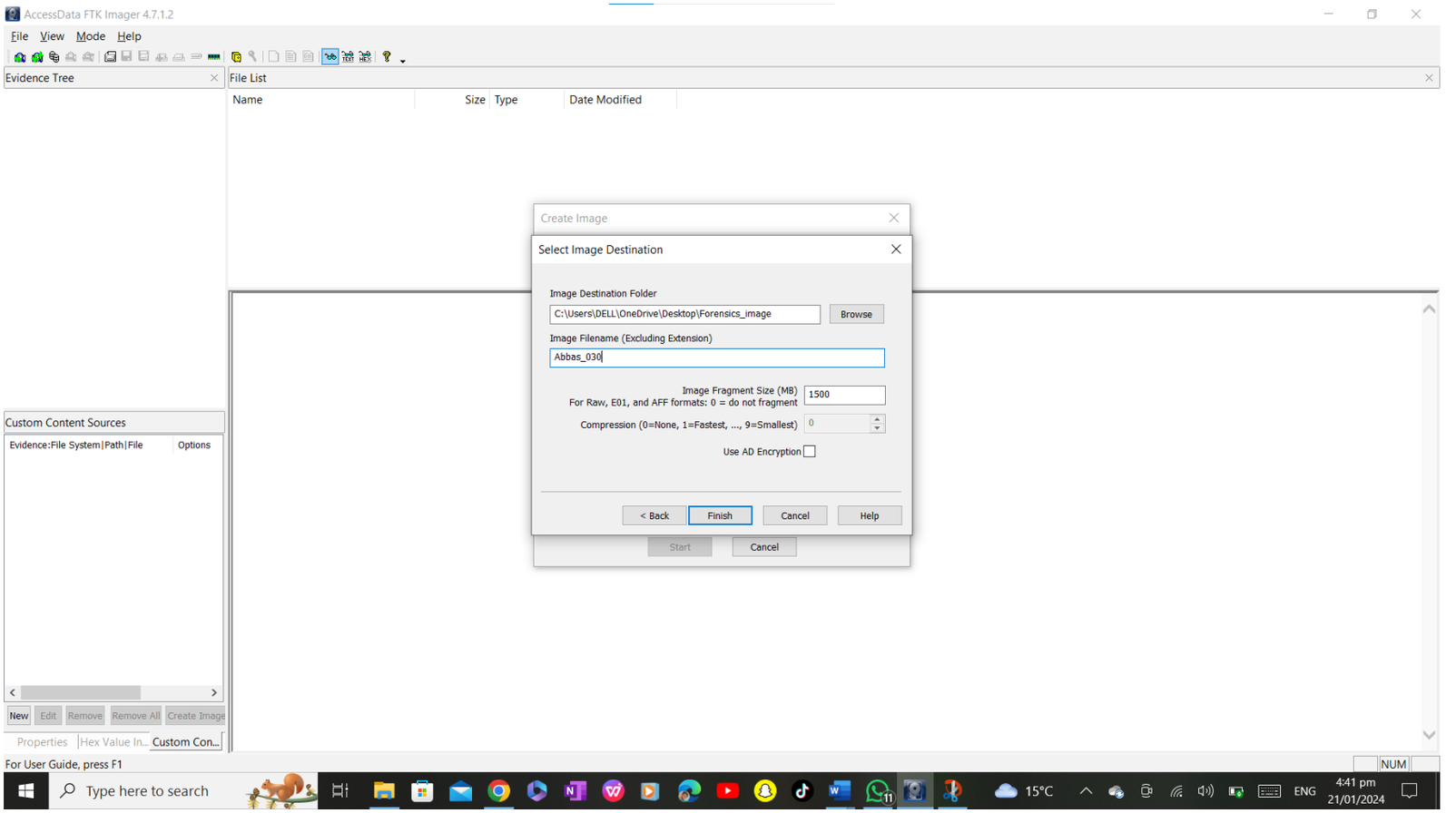


Select the destination drive or folder where you want to store forensic image.

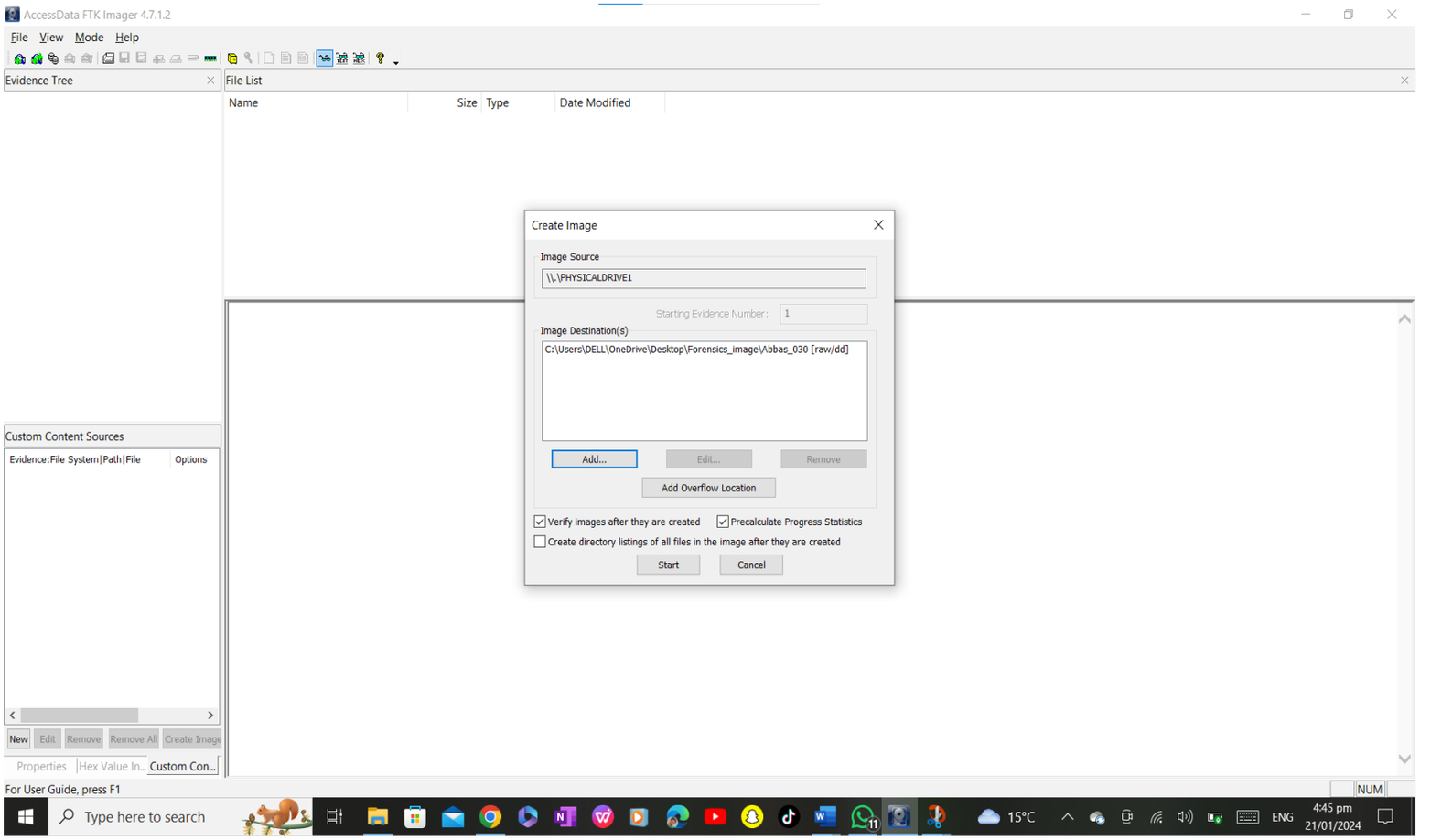
Note: Make sure destination drive is larger than source drive.



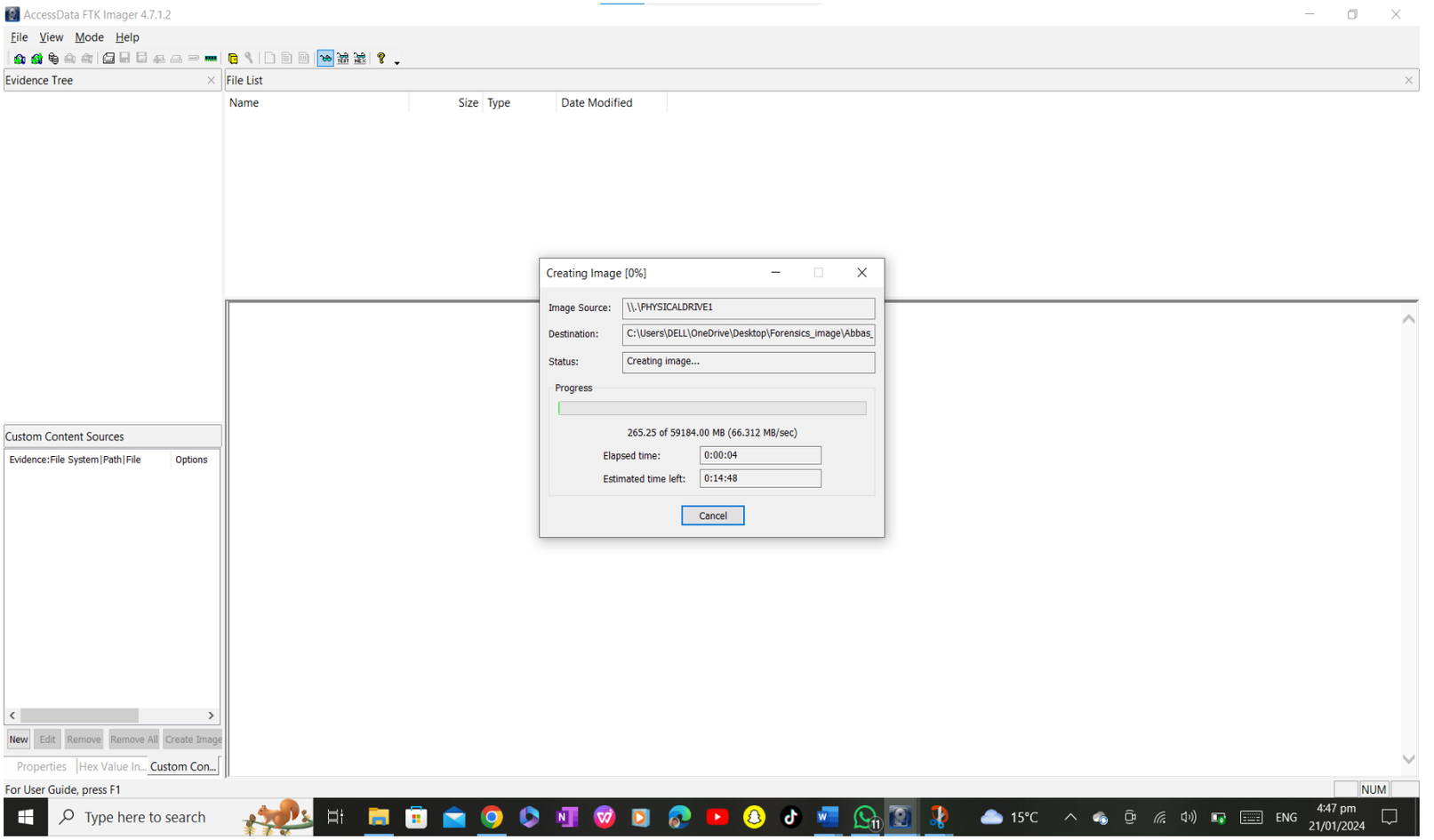
Select the destination for the image and Name your forensic image and add fragment size in Mega Bytes.



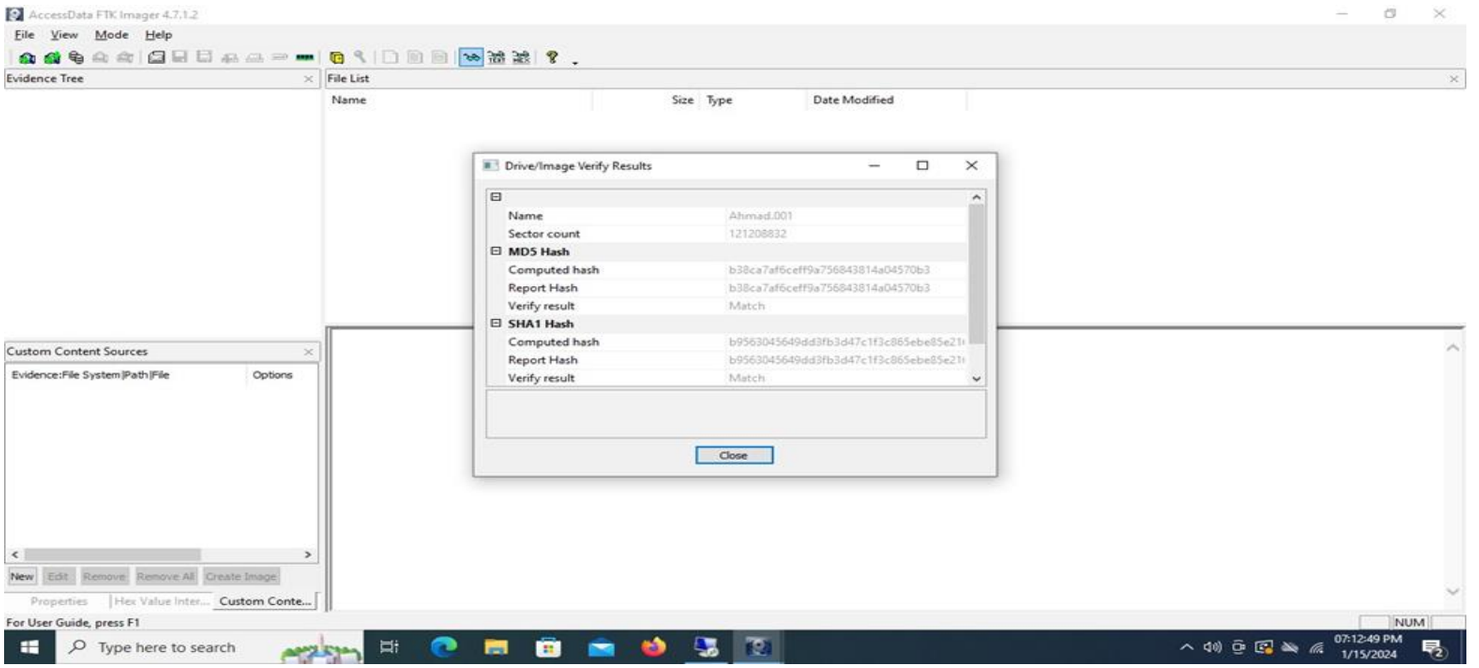
Here, we are starting the process for creating the forensics image.



The process has started



The Image has created

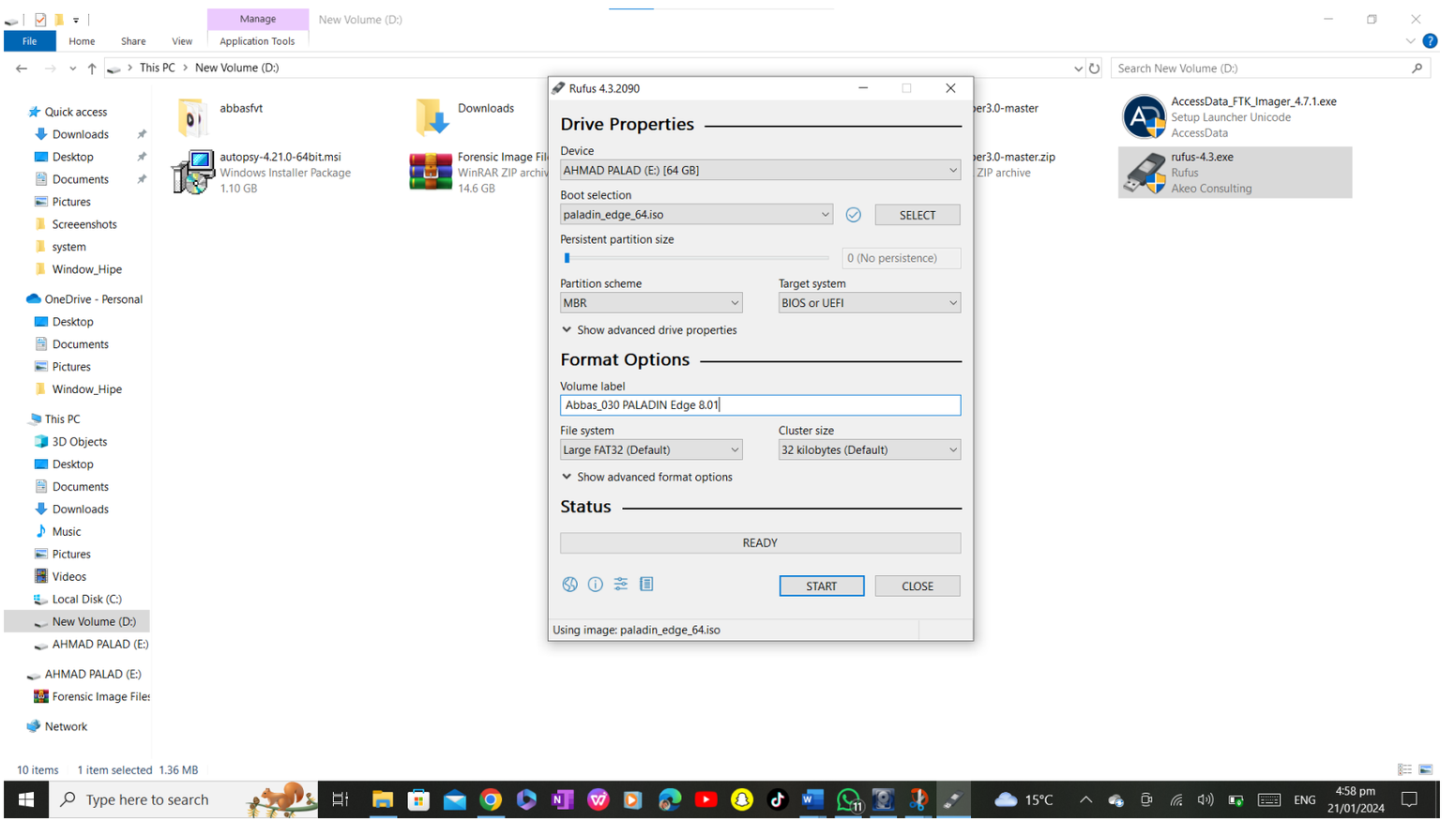


Question 3: Explain how you can create live bootable USB using Paladin ISO file and state the main features of using Paladin (Situation-ii)

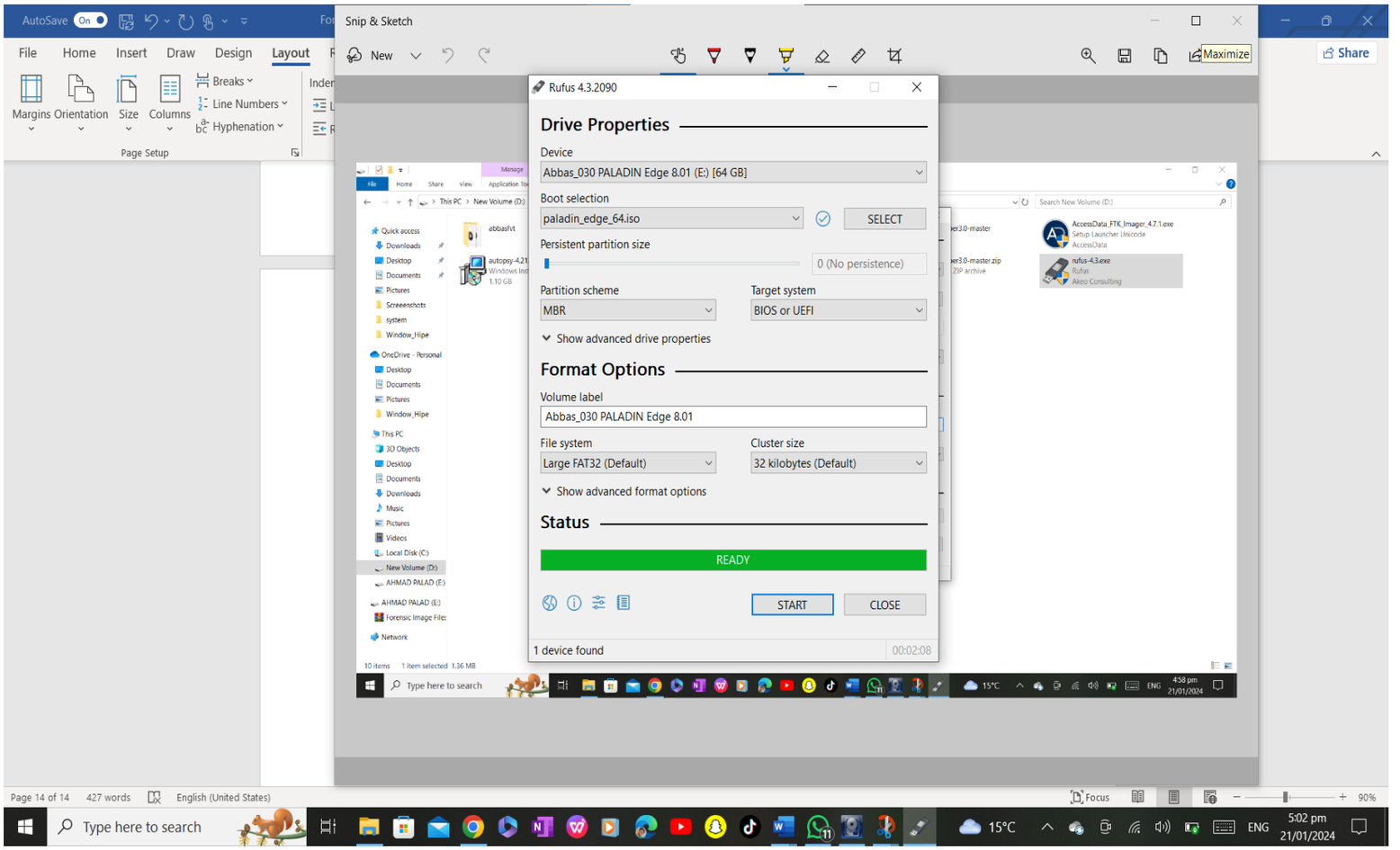
Answer: First open rufus software or any other software used to create live bootable USB. Select the USB.

Write name for your device l.

Select File system. NTFS or Fat32. Click start and your device will be ready.



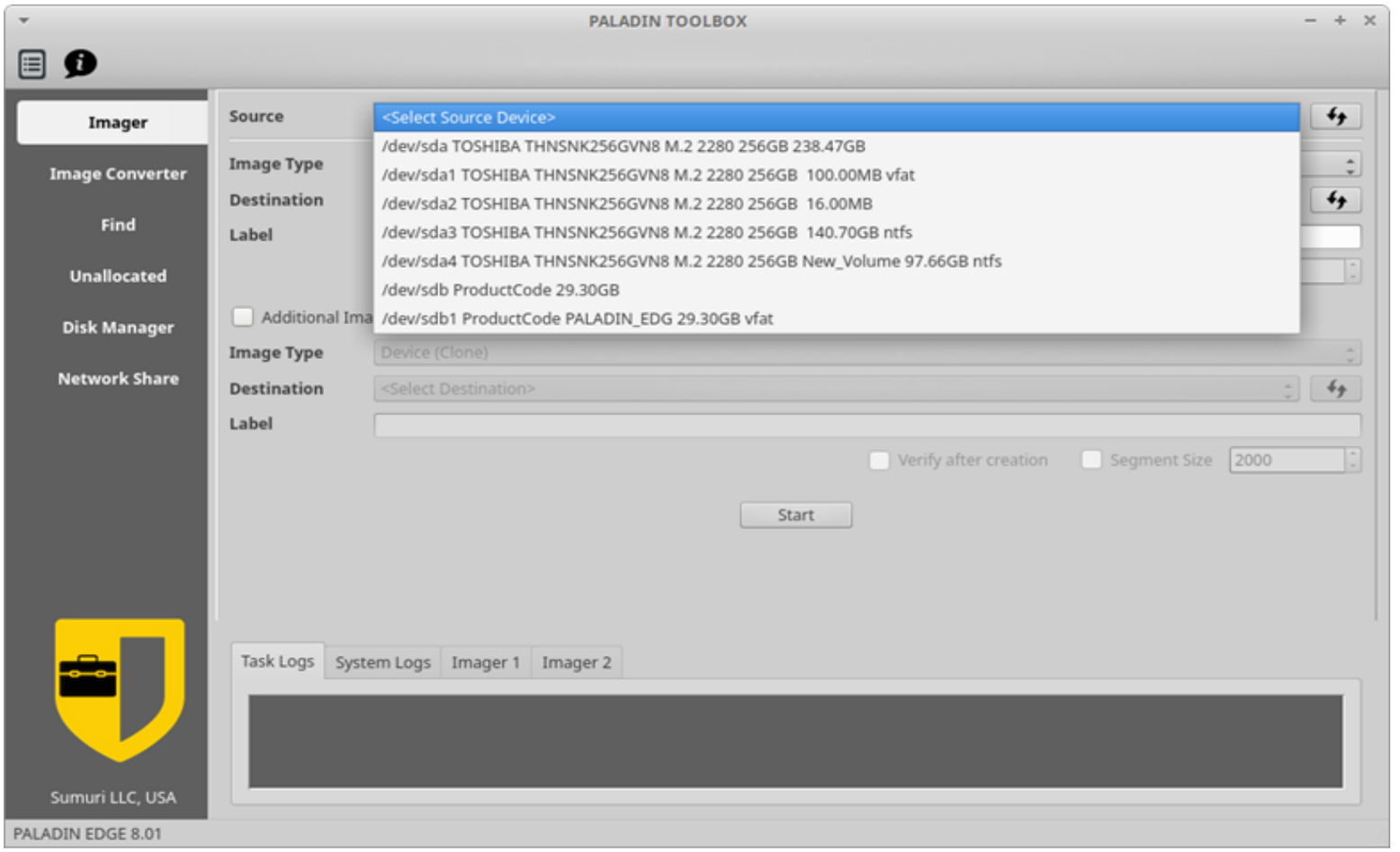
Paladin is ready now restart the laptop and press F12 when the screen will of.



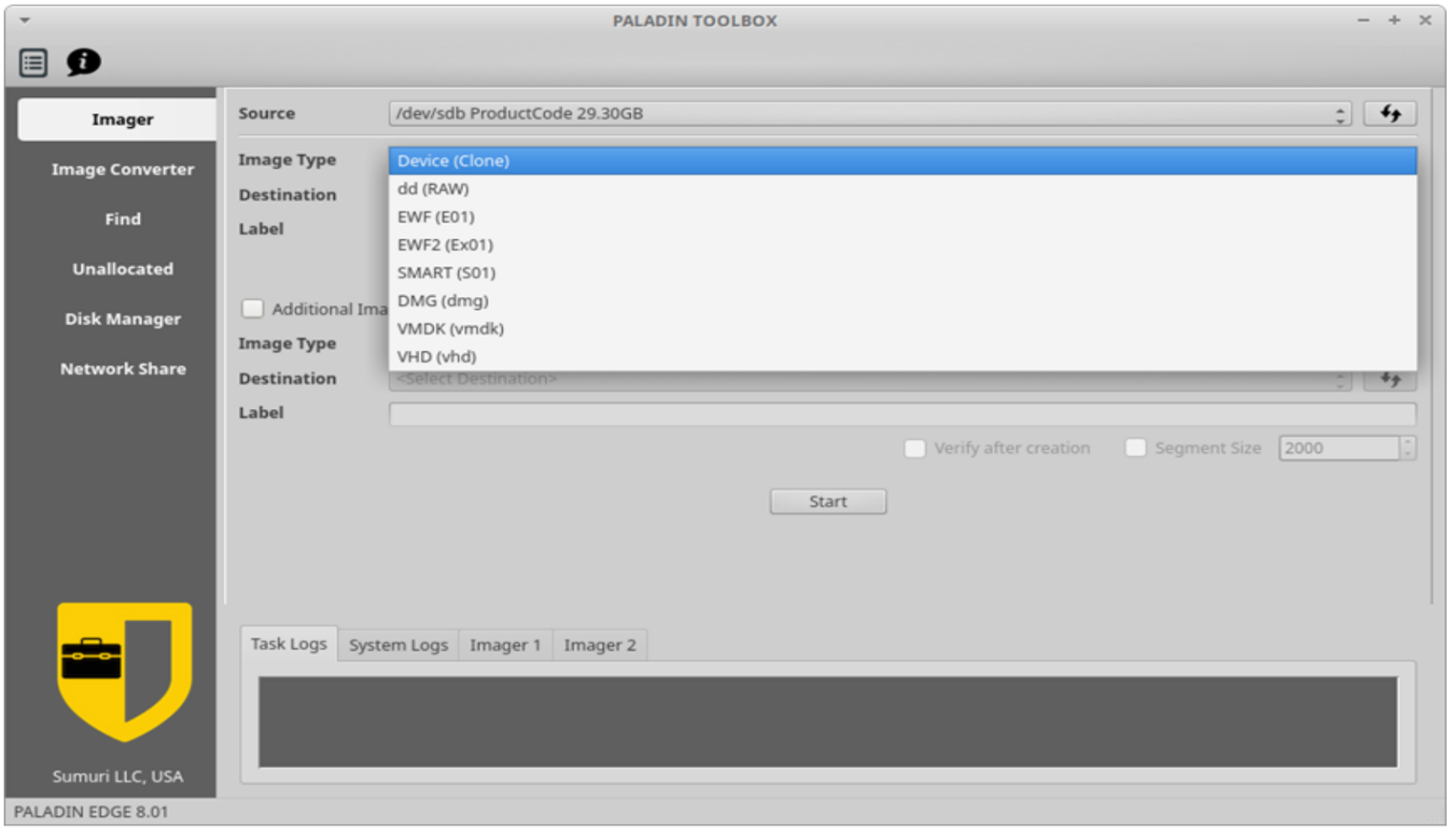
Question 4: Create forensic image of any source device of disk/USB/SD cards etc. with title of your name using the prepared live bootable Paladin forensic tool (situation-I).

Ans: Open Paladin from live bootable USB.

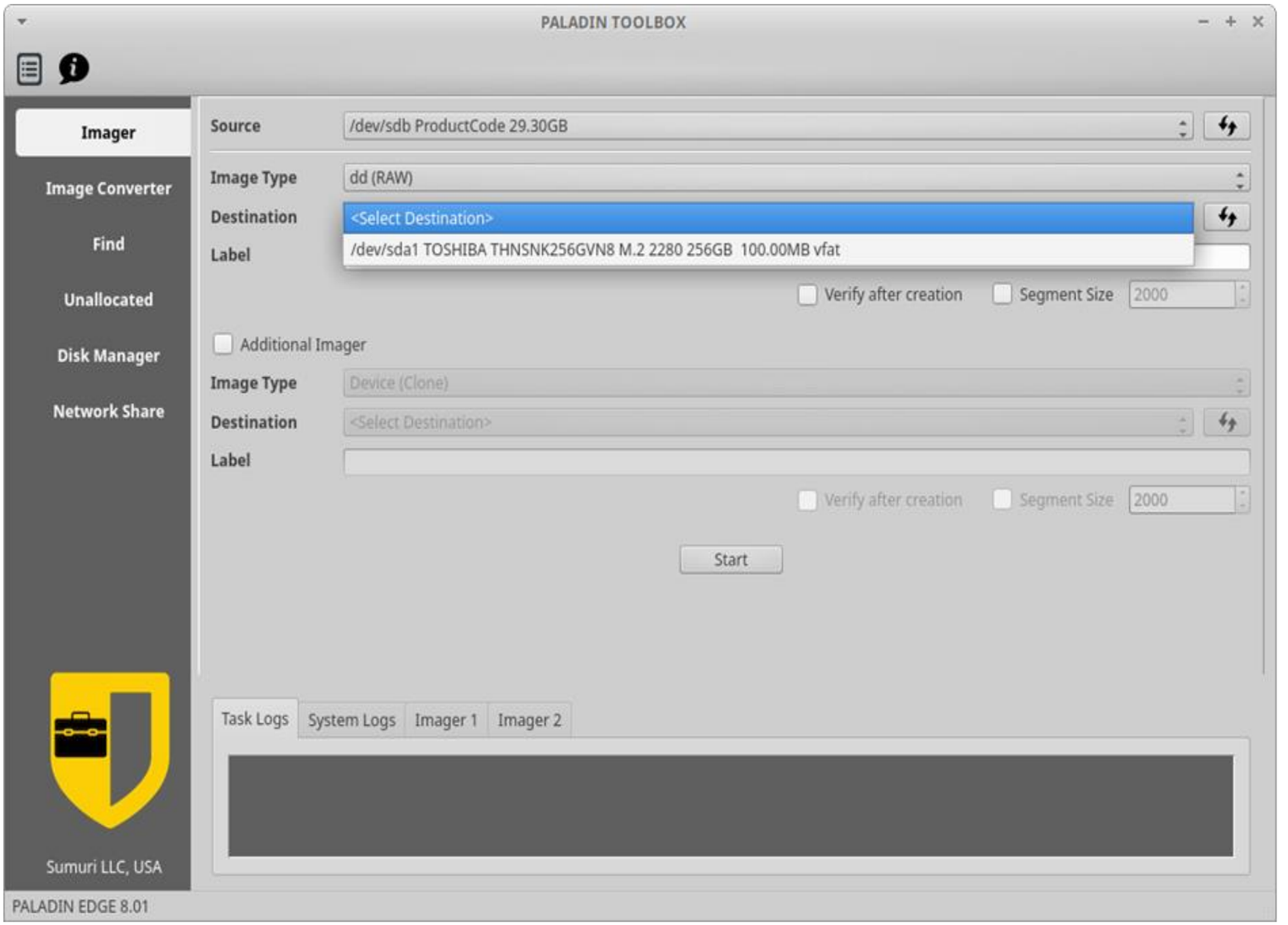
Then Select “Source Device” from the drop-down menu



Chose image type.



chose destination and mark a segment size.



click start and the image will be created.